UNIVERSITÉ DE MONTRÉAL

IMPROVEMENT OF RISK ALLOCATION METHODS AND CHOOSING PL AND SIL FOR SAFETY FUNCTIONS IN MACHINE INDUSTRY BY USING FUZZY LOGIC

MOHAMMAD SOHANI
DÉPARTEMENT DE MATHÉMATIQUES ET DE GÉNIE INDUSTRIEL
ÉCOLE POLYTECHNIQUE DE MONTRÉAL

MÉMOIRE PRÉSENTÉ EN VUE DE L'OBTENTION
DU DIPLÔME DE MAÎTRISE ÈS SCIENCES APPLIQUÉES
(GÉNIE INDUSTRIEL)
AVRIL 2013

UNIVERSITÉ DE MONTRÉAL

ÉCOLE POLYTECHNIQUE DE MONTRÉAL

Ce mémoire intitulé :

IMPROVEMENT OF RISK ALLOCATION METHODS AND CHOOSING PL AND SIL FOR SAFETY FUNCTIONS IN MACHINE INDUSTRY BY USING FUZZY LOGIC

présenté par : SOHANI Mohammad
en vue de l'obtention du diplôme de : Maîtrise ès sciences appliquées
a été dûment accepté par le jury d'examen constitué de :

M. AGARD Bruno, Doct., président
M. CHINNIAH Yuvin, Ph.D., membre et directeur de recherche
M. OUALI Mohamed-Salah, Doct., membre et codirecteur de recherche
M. TURCOT Denis, M.Sc.A, membre

To my lovely wife, Maryam...

RÉSUMÉ

La précision par rapport à la répartition des risques et aux étapes de validation est indispensable pour appliquer la norme ISO 13849 concernant la sécurité des systèmes de contrôle. Toutefois, les données de taux d'échecs sont rarement fournies aux concepteurs et également généralement non-fournies avec composants utilisés dans les systèmes de sécurité. Plus récemment, les entreprises commencent à mesurer les taux d'échecs et incluent ces taux dans leurs fiches techniques. Pendant ce temps, d'autres sources pour les données peuvent être utilisées, et englobent les données inconnues et erreurs provenant de différences entre environnements de tests et d'application/intégration réelle. Les méthodes conventionnelles utilisées pour normes utilisant des niveaux spécifiques ne sont pas appropriées dans ce cas. De plus, la méthode d'évaluation des risques utilisée pour définir le niveau de performance requis («PLr») pour le système de contrôle de sécurité utilise l'avis d'experts pour définir les niveaux de risque des composants. L'utilisation d'avis d'experts entraîne des problèmes reliés à la subjectivité et les valeurs spécifiques ne sont pas appropriées pour exprimer l'évaluation adéquate des risques. L'application de la logique floue pour la norme peut résoudre ces deux problèmes. La logique floue est réputée de traiter efficacement les cas comprenant l'incertitude et la subjectivité. La logique floue peut améliorer la méthodologie et réduire les allocations supplémentaires en matière de conception.

En utilisant la théorie d'ensembles flous, deux problèmes majeurs en appliquant les deux normes de sécurité, ISO 13849 et IEC 62061, peuvent être résolus dans une certaine mesure. Le premier problème lors de l'application de ces normes se relie aux différentes approches utilisées par chaque norme pour définir les niveaux de sécurité requis et obtenus pour systèmes de contrôle. ISO 13849 utilise des niveaux de performance («PL») et IEC 62061 utilise des niveaux d'intégrité de sécurité («SIL»). Bien que les niveaux de sécurité pour ces deux paramètres sont basés sur la probabilité de défaillance dangereuse par heure, les méthodologies utilisées pour définir les niveaux sont différentes. En attribuant des valeurs linguistiques basées sur des ensembles flous et utilisées pour définir des niveaux pour les paramètres de risque, ceci par conséquent peut aider dans la conception d'une méthode de répartition dont les résultats sont plus comparables aux deux approches. De cette façon, les niveaux de sécurité provenant de la nouvelle méthode de logique floue peuvent être utilisés par les deux normes de sécurité et résolvent le problème lié aux écarts entre les résultats des deux méthodes. L'avantage de l'approche de logique floue est que cette nouvelle méthode peut s'appliquer (est en conformité) avec les deux normes. De plus, l'utilisation d'avis d'experts en tant que

source exclusive d'informations pour définir les niveaux de sécurité d'un système de contrôle s'avère d'être une méthode trop complexe et subjective. Par conséquent, l'extraction d'informations utiles nécessite une méthodologie formelle. La méthode de logique floue est utilisée dans cette étude et sert à transférer les informations d'experts à un modèle mathématique qui est ensuite utilisé pour définir les niveaux de sécurité.

ABSTRACT

Precisions of risk allocation and validation steps are essential to apply standard ISO 13849 on safety related control systems. However, failure rate data is rarely available to designers and usually not provided with components used in safety systems. Recently, companies have started to perform measurements for failure rates in order to include them into their data sheets. Meanwhile, other data sources may be used which encompass uncertainty and error due to dissimilar specifications between test and implementation environment. Conventional methods used in standards based on crisp levels are not appropriate in this respect. Additionally, risk assessment method employed to define required performance level (PLr) for the safety control system uses expert's opinion to define risk component levels. Using expert's opinion entails subjectivity problem and crisp values are not appropriate to express judgmental risk assessment. Applying fuzzy logic in the standard can solve both these problems. Fuzzy logic has been proven to deal effectively with uncertainty and subjectivity. It can improve the methodology and reduce overdesign possibility.

Using fuzzy set theory two major problems in using the two safety standards, ISO 13849 and IEC 62061, can be solved to some extent. First problem in using these standards is the different approaches they use to define required and achieved safety level for safety related control systems. ISO 13849 uses performance levels (PLs) and IEC 62061 uses safety integrity levels (SILs). Although safety levels in both parameters are based on probability of dangerous failure per hour, methodologies used to define levels are different. Reassigning linguistic values based on fuzzy sets, used in defining levels in risk parameters, can help to design an allocation method which its result is more comparable to both approaches. This way, safety level from the new fuzzy method may be used by both safety standards and ultimately solves the problem of discrepancy between results from two methods. The advantage of fuzzy approach is that the new method is in accordance with both standards. Additionally, the employment of expert's opinion, as the only source of information, in defining safety level for a safety related control system is inherently subjective and complex. Therefore, elicitation of useful information requires a formal methodology. Fuzzy method is used in this paper to transfer information from experts to a mathematical model, which then is used to define safety levels.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ACRONYMS AND ABBREVIATIONS

PLC	Programmable Logic Controller
SRCS	Safety Related Control Systems
PL	Performance Level
E/E/PE	Electrical/Electronic/Programmable Electronic
SIL	Safety Integrity Level
FB	Function Blocks
CF	Control Function
CCF	Common Cause Failure
MTTF	Mean Time To Failure
$MTTF_d$	Mean Time To dangerous Failure
DC	Diagnostic Coverage
DC_{avg}	Average Diagnostic Coverage
PL_r	Required Performance Level
PFH	Probability of Failure per Hour
PFH_d	Probability of Dangerous Failure per Hour
PFD	Probability of Failure on Demand
SFF	Safe Failure Fraction
SRC	Safety Related Control

LIST OF APPENDICES

CHAPTER 1

INTRODUCTION

A major number of deaths around the world and in Canada are caused by occupational accidents [5]. As a result, occupational safety have received much attention. Specifically, countries in the European union have paid much attention and introduced laws and regulations over industries to prevent occupational diseases and accidents. As an example, all companies in Europe are required to apply requirements of machine directives [6]. Not only occupational safety can decrease potential harm to human, it may also decrease dramatically the resulting costs. Total cost of occupational accidents and injuries is estimated around 4% of the national product [7]. In Canada, only in 2005, 1097 workers were killed and around 335000 were injured or suffered from accidents at work, which resulted to seven billions of dollars expense for the government and companies [8]. Surprisingly, only in Quebec around 13000 of these accidents were caused by machines which make safety an inevitable requirement for industrial machines.

A major step in finding safety requirements for a machine is to perform risk assessment. It has been shown that about 40% of faults related to programmable electronic systems are because of underestimated risk assessment [9]. Consequently, if the safety level is not adequate, further actions have to be taken. A very popular risk reduction method is using guards to limit access to hazards. However, before doing risk reduction by using guards, all efforts have to be made to remove the hazards by intrinsic design or application of good engineering practice. Unfortunately, due to the engineering costs and limitations, it is not always possible to do risk elimination by intrinsic safe design. If it is not possible to eliminate a hazard through safe design, risk reduction process has to be continued until an acceptable safety level is reached by using other practical approaches [10]. Functional safety defined as, part of the machine control system which depends on the correct functioning of the safety related control system and external risk reduction facilities [3], has been proven to be an effective method to increase safety in industrial machines [11].

Figure 1.1 shows a safety problem deploying functional safety. A machine with a rotating component is to be secured by means of a safety door so that whenever the door is opened, the rotating part stops. A sensor detects status of the door. When the door is opened, meaning that a dangerous situation is produced, sensor sends a signal to existing logic. The logic

circuit then stops the machine by disconnecting the power to the rotating part of machine. This can be implemented in different safety levels and by using different technologies.

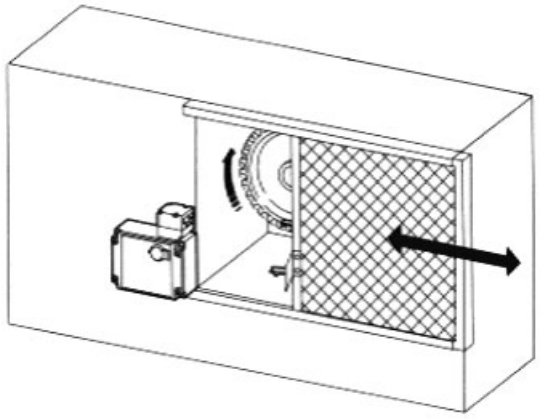


Figure 1.1 **Safety control system stops rotation when safety guard, protecting rotating part of machine, is opened**

To regulate safe machine design and to ensure that required safety level for a machine is met, various standards have been introduced. In ISO 14121 [12], the hazard identification and risk estimation procedures are described and risk evaluation for each hazard is discussed in details. The EN ISO 12100 [13] , which now includes ISO 14121, introduces basic concepts and principles required to design a safety system and includes principles for risk assessment and risk reduction. The first standard on designing safety control systems for industrial machines is EN 954-1 [14]. It includes all the basic requirements later used in other standards.

The EN 954-1 uses categories to describe integrity level of safety control function. Depending on the results from risk assessment and the expectation from safety control, a category is chosen for the safety function. The categories describe the structure of safety related control system by using fault tolerance of the whole safety control function and how effectively tests can find faults. A breakthrough by introduction of EN 954-1 was that categories were based on control system's performance and safety parts of control system could be used independently from their technology. This means that electrical safety control systems may be used in combination to other technologies such as hydraulic and mechanical.

First, dependency of functional safety on control system is verified. If there is no need to use control system, design can be continued using other risk reduction methods. If control is required, then an iterative design will be started by identifying the safety function and its characteristics. Following full definition of the safety function, the required performance level

will be determined using appropriate risk assessment method. Safety standards use different approaches to assign required safety integrity level or performance level to a safety control system and as shown later, this may end up to inconsistent results.

The next standard over safety control systems, EN ISO 13849-1:2006 [2], describes the required steps to design and integrate hydraulic, electronic and mechanical safety related parts of control system and protective devices. The concept of performance levels, introduced in this standard, can be viewed as an enhancement of categories which are known from the older version, EN 954-1. Together with Part 2 of standard–EN ISO 13849-2:2003 [15], EN ISO 13849-1:2006 replaces EN 954-1.

Another existing standard on machine safety control system is IEC 62061 [3]. It is aimed only for electrical, electronic and programmable (E/E/PE) safety related part of control system (SRCS). If the control system includes hydraulic or mechanical system, ISO 13849 has to be used for non-electrical/electronic parts. The design methodology used in IEC 62061 covers complex as well as simple structured system. It starts using machine's life cycle and continues by dividing up to down the design of E/E/PES safety system. Similar to its generic version, IEC 61508, IEC 62061 uses safety integrity levels ($SILs$) to show the level of performance and to classify safety system.

The structure of this thesis is as follows. In next section, a brief review of safety standards and their methodologies are presented. It emphasizes definition of problems studied in this thesis and a literature review on what has been done. Section.3 then introduces the contribution of each one of writer's papers and Section.4 gives a brief conclusion.

CHAPTER 2

PROBLEM DEFINITION

2.1 Standards over safety control systems in machine sector

Today, an important part of any safety control system is Electrical, Electronic and Programmable Electronic (E/E/PE) devices. The existing standards on safety control, namely IEC 62061 and ISO 13849-1, set rules on design, implementation and validation of safety system to fulfill a required level of integrity. Risk level allocation constraints the minimum required level of safety. Then safety control system has to be designed using standard's directives. Afterwards, the achieved integrity is verified versus required specifications and probability of dangerous failure per hour (PFH_d). Each of the two standards have its own measures to achieve an integrity level.

In ISO 13849, risk allocation uses crisp levels to assign required level based on expert's opinion, which is not crisp in nature. Additionally during validation step, non crisp MTTF_ds are mapped to crisp levels to be used in simplified method. The problem is that at each one of these steps a level of estimation exists and values are rounded up toward safe side and this may result to overdesign problem. The second problem is in having two safety standards valid at the same time. The risk allocation, which defines requirements of a safety function can be evaluated to different levels in ISO 13849 and IEC 62061. The following sections study methodologies used in these two standards including the above mentioned problems.

2.1.1 Risk allocation and validation in ISO 13849

All machines in European territory have been required to follow safety directive after 1996. For safety control systems, the safety standard EN 954-1:1996 has been used as a directive. Using EN 954-1 continued with success for around a decade. It was rather easy to understand and to apply. Since machines have been improved and new technologies have been used in industry to build more and more complex systems, there was no question that standards had to be revised.

It was in 1999 when ISO published a new standard in which probabilistic methods were used in addition to previous qualitative measurements. Besides, new quantitative measurements

were added to increase integrity. These measurements are based on probability of dangerous failure per hour.

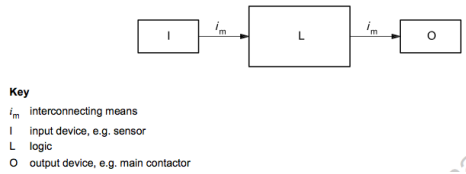
The quality of safety related control system in ISO 13849-1 is indicated by five Performance Levels (PLs). These five levels are related to PFH_d as shown in Table 2.1. These levels set the maximum reachable level for a safety function. To ensure reaching the required level of safety, other measurements such as resistance to CCF and systematic failure are required.

Table 2.1 Performance Levels used in 13849-1 and corresponding PFH

Performance Level (PL)	**Average probability of a dangerous failure per hour (PFH) in h^{-1}**
a	$1 \times 10^{-5} \leq x < 1 \times 10^{-4}$
b	$3 \times 10^{-6} \leq x < 1 \times 10^{-5}$
c	$1 \times 10^{-6} \leq x < 3 \times 10^{-6}$
d	$1 \times 10^{-7} \leq x < 1 \times 10^{-6}$
e	$1 \times 10^{-8} \leq x < 1 \times 10^{-7}$

'x' shows resulted PFH

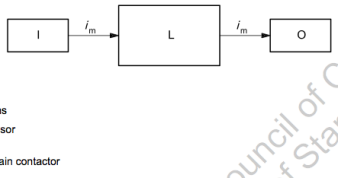
Using probabilistic methods causes difficulties, specifically in small companies. Using these measurements means that required specifications of design have to be defined based on these values and afterwards design has to be verified against them. In order to make analysis easier, 13849-1 introduced five design structures, each related to one PL. Designated architectures suggested in ISO 13849 are depicted in Figure 2.1. If one of these architectures is used, performance level and consequently probability of dangerous failure per hour may be calculated using the simplified proposed methodology. Otherwise, other modeling approaches such as Markov shall be used which requires complex calculations and consequently more effort. Figure 2.2 shows proposed design process step by step.



Key

i_m interconnecting means
I input device, e.g. sensor
L logic
O output device, e.g. main contactor

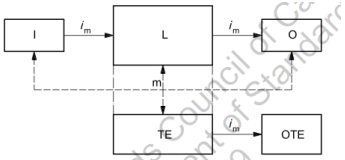
(a) Designated architecture in ISO 13849-1, Category B



Key

i_m interconnecting means
I input device, e.g. sensor
L logic
O output device, e.g. main contactor

(b) Designated architecture in ISO 13849-1, Category 1

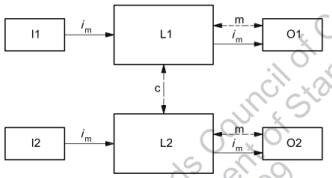


Dashed lines represent reasonably practicable fault detection.

Key

i_m interconnecting means
I input device, e.g. sensor
L logic
m monitoring
O output device, e.g. main contactor
TE test equipment
OTE output of TE

(c) Designated architecture in ISO 13849-1, Category 2

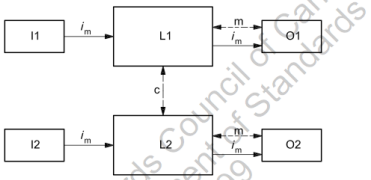


Dashed lines represent reasonably practicable fault detection.

Key

i_m	interconnecting means
c	cross monitoring
I1, I2	input device, e.g. sensor
L1, L2	logic
m	monitoring
O1, O2	output device, e.g. main contactor

(d) Designated architecture in ISO 13849-1, Category 3



Solid lines for monitoring represent diagnostic coverage that is higher than in the designated architecture for category 3.

Key

i_m	interconnecting means
c	cross monitoring
I1, I2	input device, e.g. sensor
L1, L2	logic
m	monitoring
O1, O2	output device, e.g. main contactor

(e) Designated architecture in ISO 13849-1, Category 4

Figure 2.1 Designated architectures in ISO 13849-1

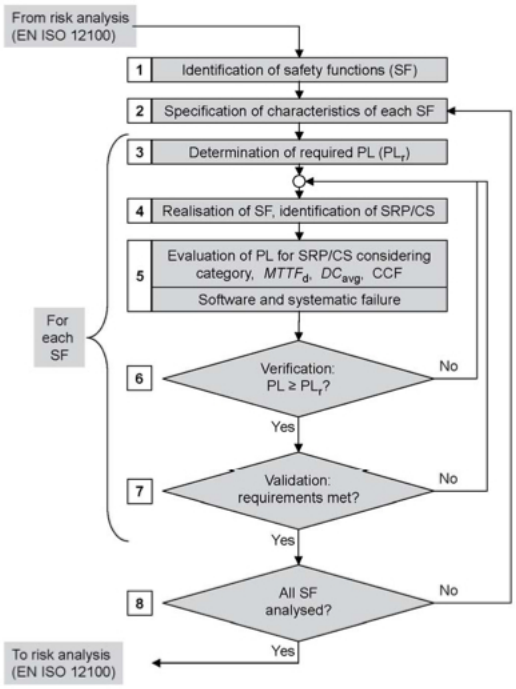


Figure 2.2 Design process used in ISO 13849-1 [1]

Based on risk allocation done on the machine, a performance level is required (PL_r) and consequently a category is chosen appropriate for that PL_r. Each category is assigned to one designated structure. These structures only show logical relation and do not represent detailed design. It is evident that to design a safety function, one has to be skillful and experienced to follow steps in ISO 13849-1:

1. *Identification of safety functions (SF):* At this step, we already know what dangerous phenomena exist in the machine. Thus, we have to define safety functions that, if implemented properly, can secure existing dangerous phenomena and reduce risks to an acceptable level. For example, to secure a press which is fed manually, we may secure backside by interlocking guard and front side by a light curtain.
2. *Specification of characteristics of each SF:* At this step, all requirements of each SF have to be defined in detail. For example, for the interlocking guard, the guard is supposed to be locked whenever machine is running. If door is opened in the running mode, machine has to be stopped immediately and not started until it is checked and restarted manually.
3. *Determination of required PL (PL_r):* The required PL can be determined based on severity of accident, exposure frequency and probability of avoidance from risk (see

Figure 2.3).

4. *Realization of SF, identification of SRP/CS:* Now that PL_r is determined, the SF can be implemented based on its specification and required measurements to satisfy PL_r. At this stage, an appropriate design structure based on PL_r is chosen and then components are chosen and implemented such that they fulfill all measurements such as DC_{avg}, etc. This is where using simplified method can be helpful.
5. *Evaluation:* The designed safety function should be verified using measurements versus performance level. If the measured performance level is smaller than PL_r then design has to be changed using one or more of the following options:
   – Using redundant components
   – Using diagnostic coverage to improve dangerous undetected failure rate
   – Using a higher performance component to improve failure rate

It is required that a performance level be specified as the target value for each safety function. This requirement is derived from the risk reduction that is necessary to reach target safety level. Among values and aspects which are considered to determine the required performance level, likelihood and severity of accident are important measures. ISO 13849 uses risk graph to determine required performance level.

Graphical risk allocation (risk graph - Figure 2.3) is a method to calculate the required performance level using risk parameters. The following risk parameters are required to be evaluated as part of risk graph PL determination:

– S: Severity of injury
– F: Frequency and time of exposure to hazard
– P: Possibility of avoiding the hazard or limiting the harm

The graphical safety level allocation must be performed for each safety function without considering other risk reduction approaches. In general, the severity of injury at hazardous zone varies widely, however, for control system's requirements using ISO 13849 only two levels are relevant:
– S1: Slight (normally reversible injury)
– S2: Serious (normally irreversible injury)
The frequency of exposure to hazard are evaluated to have:
– F1: Seldom-to-less-often and/or exposure time is short
– F2: Frequent-to-continuous and/or exposure time is long
It has to be noted that a clear boundary does not exist between F1 and F2. Based on an instruction in the standard, in cases where operator intervenes more than once per hour, F2

is more appropriate than F1. However, for a case where machine is setup once per year and then operates automatically, the choice of F is not clear enough [1].

The possibility of avoiding the hazard P, is determined to be:
– **P1:** possible under specific conditions
– **P2:** scarcely possible
To define this parameter, physical characteristics of the machine and possible reaction of the its operator shall be determined. As an example, if the machine has the characteristic which forces speed limit during its operation, then P1 is more appropriate for slow speeds than P2. The reason is that lower speed gives more room to the operator to move out of the hazardous area. On the contrary, P2 is the right choice when high acceleration does not give enough opportunity to the operator to evade an accident.

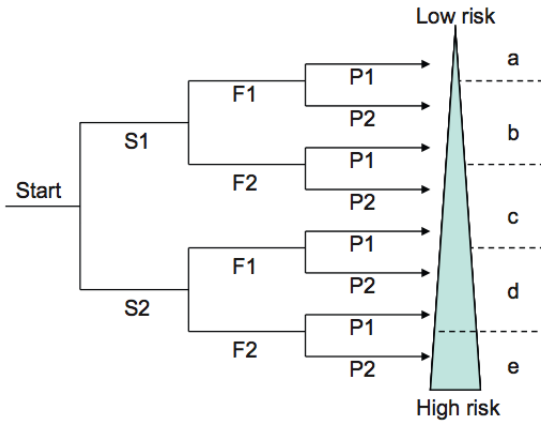
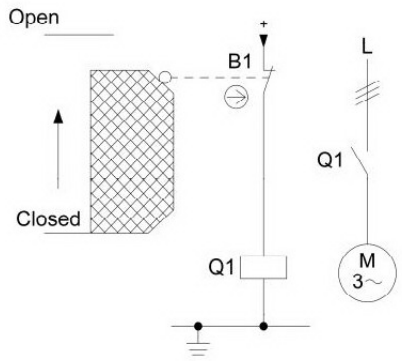
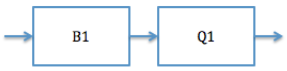


Figure 2.3 Graph method to estimate the required performance level (PL_r) [2]



(a) Safety door. Example taken from BGIA report on ISO 13849-1 [1]



(b) Reliability circuit

Figure 2.4 Safety function with PL=b based on ISO 13849 for the example in Figure 1.1

Risk Parameters:

S: Severity of injury

S1: Slight (normally reversible injury)

S2: Serious (normally irreversible injury)

F: Frequency and/or exposure to hazard

F1: Seldom-to-less-often and/or exposure time is short

F2: Frequent-to-continuous and/or exposure time is long

P: Possibility of avoiding hazard or limiting harm

P1: Possible under specific conditions

P2: Scarcely possible

Figure 2.4a shows an example for a safety door designed at category 1 based on ISO 13849 and figure 2.5 illustrates associated PL allocation. The safety function is a stop function, initiated by a protective device. When the movable part (here door) opens, a stop function will be initiated causing movable part of the machine to stop. A switch (B1) detects opening of the movable guard and then contactor Q1 will disconnect power to the motor. This prevents movement of hazardous part of machine.

First a required performance level has to be allocated to this safety function. The first

risk parameter to be determined is the severity of injury (S). S is equal to $S1$ for slight injuries (normally reversible). Using this definition, a broken finger or broken hand should be assigned to $S1$, while this can also be assigned to bruising or even small cuts. Boundaries between levels used in graphical risk allocation are not clear. Using adverbs such as normally, frequently, seldom and etc. makes these boundaries more vague. Can we associate a broken rib or hand to S2? What does normally (ir)reversible mean? Wouldn't it more proper for an expert to have a scale between these two values, so that s(he) could assign a value between S1 and S2 to such injury?

The next risk factor is frequency and/or exposure to hazard (F). Supposing that the frequency of exposure to hazard more than twice per hour, F should be equal to $F2$. However, not all situations are this obvious. For values between once per hour and once per year, clear definition does not exist. Expert can interpret adverbs such as frequent or seldom to the extent he/she has experienced. The last risk parameter is easier to be determined. The possibility of avoiding or limiting harm can be determined as P1 for possible situations and equal to P2 for scarcely possible situations. However, using scarcely can again be interpreted by the expert.

Most risk evaluation (safety integrity allocation) methods are based on the same concept of using severity and occurrence with different level of precision in defining description of risk parameters. While various approaches exists, all suffer from the fact that using expert's opinion is imprecise, uncertain and prone to error (Sandri [16] and Hietikko [4]). Most importantly, in graphical risk allocation of ISO 13849, expert has to choose between two levels while descriptions for such levels are not always precise and helpful. As such, expert may interpret description based on his/her experience. What if expert doubts which risk level is applicable? What if situation does not match any of the descriptions?

In choosing a level for risk parameter, there are situations where none/both descriptions match the situation. In such cases, expert has to choose higher risk level to keep the safe side of design. It is not clear how frequently and continuous should be interpreted. In such cases, expert has to choose the higher risk level and this may result to over-design. Thus, it is appropriate to minimize such limitations in order to achieve more precise risk assessment.

Thus, the following technical issues in using ISO 13849 exist:
- Expert opinion is used to estimate discrete risk paramter levels which is not appropriate.
- Performance levels are discretized version of PFH_d values, while MTTFd and DCavg are not discrete. Consequently, validation of designed safety function requires comparison of discrete values versus continous values.

,

The paper (see Appendix A) suggests using Fuzzy to solve this problem. First reason is that fuzzy can be used to interpret linguistic values such as: scarcely, frequent, etc. It has also been shown that presentation of opinion using values in a range is more appropriate for experts (see Sandri[16]). Another advantage of using fuzzy is that fuzzy risk allocation can generate results as PFH, which can be used directly in validation step to further decrease the chance of over/under design.

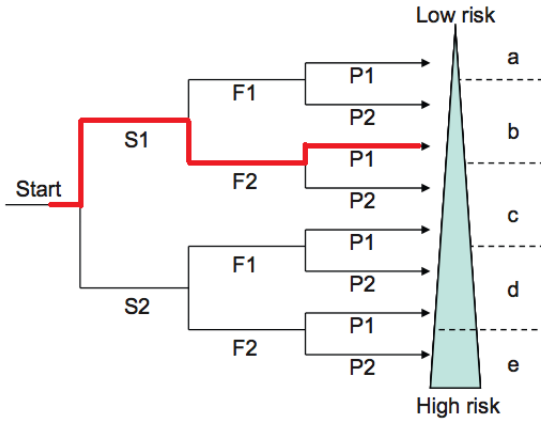


Figure 2.5 Allocation of PL to safety function in the example

After designing a SF, result has to be validated to confirm that it fulfills the required performance level (PL_r). This will be done by considering category, required MTTF, average diagnostic coverage and common cause failure and using the method in Figure 2.6.

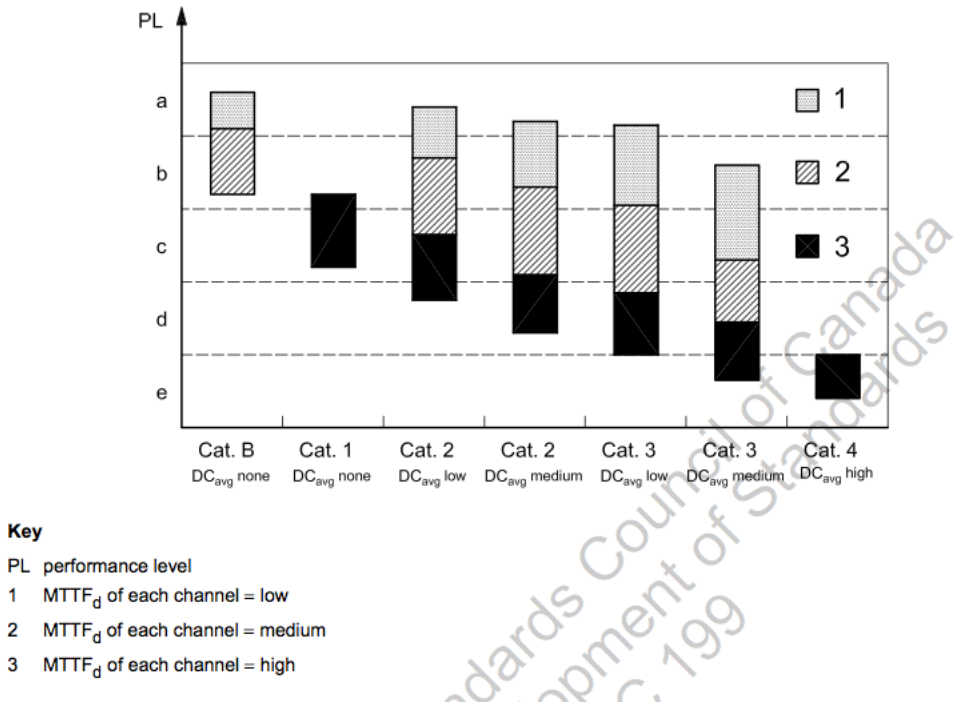


Figure 2.6 Simplified validation: relationship between Categories, DC_{avg}, $MTTF_d$ of each channel and PL

A very important task in using safety standards, is to find reliability data for safety components to calculate $MTTF_d$. Existing sources are: manufacturer's data-sheet, military data book, life-testing program in company, data in standards or other publications that include components failure data, such as MIL-HDBK-217F, IEC/TR 62380, NPRD 95 or IEC 61709. It is not questionable that the preference is to use manufacturer data. Since in some sectors, it takes time to provide such data, some components do not yet have these information from their manufacturers. Examples are hydraulic components. But, there is an increasing trend to provide reliability data. Other sources of data that may be used are data collections from other sectors than machinery. At the end, the standard has a table that may be used in case that none of the above sources of information does not exist.

Diagnostic coverage also plays an important role in defining the performance level of a safety control system. If a high value of performance level is required, tests are used to reveal any existing problem in the system. In the case of problem, system may go to safe stop state or continue its job depending on the system, while the failed component is flagged for repair. To determine DC_{avg}, first diagnostic coverage for each block has to be estimated. For simplicity, standard has provided a table with most testing measures which are used in machinery. Next

step is to calculate DC_{avg} from the formula using DC and $MTTF_d$ for all blocks.

Unfortunately, the simplified method to determine attained PL employs crisp levels (see Figure 2.6). This may give false results for small errors, specially for values close to adjacent levels. Fuzzy can improve the result in using simplified method because instead of jumping between performance levels for small changes in MTTF values, changes will be smooth and instead of PLs, PFH_d can be used directly. When decision has to be made between two PLs, crisp values can give higher or lower PL than required because of a small error in MTTF or DC. In such situations, the error in over-under design is difference between two levels. Suppose that in Figure 2.5, expert chooses P2 and consequently PLc is resulted. In this case we have:

$Error = PL_c - PL_b = (10^{-6}, 3 * 10^{-6}) - (3 * 10^{-6}, 10^{-5})$

However, if all measurements are based on PFH, then instead of dealing with PLs, all we have is a PFH value. As such, even if an error exists, it is based on PFH which is in worst case equal to one performance level. Suppose that if we could estimate actual PFH_d for this safety function by another method and it was equal to $3.5 * 10^{-6}$. Then suppose that miscalculation gives a PFH_d of $2.5 * 10^{-6}$. In this case, the error would be equal to:

$Error = 3.5 * 10^{-6} - 2.5 * 10^{-6} = 10^{-6}$

Although errors in MTTF and DC can still cause the result to diverge from the real value, but this error is not as big as a performance level.

The idea is that instead of using PL, only PFH is used for allocation and validation of performance level. The result of fuzzy risk allocation is a value based on PFH while fuzzy can additionally improve how expert presents his opinion. Then result of simplified method, in PFH, is compared with risk allocation to measure the difference. If allocated probability of failure per hour is bigger than validated PFH, then safety function can be accepted, otherwise, design has to be improved.

It has been shown that fuzzy can deal with imprecision and vagueness [17] in data and also solve the problems in using crisp values [18]. We will use fuzzy logic to model the method used in ISO 13849 and compare its results to conventional methodology. Since fuzzy uses lingual values as input, it is more appropriate for use in industry.

To summarize, using fuzzy in ISO 13849 can improve:

– Risk parameter estimation: It has been shown that using intervals are more appropriate to estimate risk parameters. Fuzzy enables experts to choose a value in an interval while

using definitions from standard, can help and also solve problem of inconsistency between the results.

- Graphical PL allocation: Since linguistic descriptions are used in graphical PL allocation, risk levels are vague and can be interpreted by expert, which in turn makes them subjective in nature.
- Graphical PL allocation: Crisp levels are used to illustrate risk parameter levels, which can result to over/under estimation of PL for errors in defining risk parameters. Using fuzzy, PL allocation can be expressed as PFH values, which minimizes the error due to error in risk parameter estimation.
- Validation step: using crisp values for $MTTF_d$ and DC_{avg} values in validation step can similarly cause high over/under estimation error because of small variations in such values. Using fuzzy, all values are continuous and there is no need to discretize continuous values and increase error.

2.1.2 Risk allocation method in IEC 62061 and its comparison to graphical method

As a machine sector standard based on IEC 61508, IEC 62061 includes rules and regulations on electronic, electrical and programmable electronic control systems (E/E/PE CS) contributing in machine safety system. The safety integrity requirements for each safety related control function (SRCF) have to be derived from risk assessment applied on each safety related electrical part of control system (SRECS) to ensure the necessary risk reduction can be achieved. IEC 62061 uses Safety Integrity Levels (SILs) classification. The values related to each level show failure rate per hour (Figure 2.7).

Safety integrity level	Probability of a dangerous Failure per Hour (PFH_D)
3	$\geq 10^{-8}$ to $< 10^{-7}$
2	$\geq 10^{-7}$ to $< 10^{-6}$
1	$\geq 10^{-6}$ to $< 10^{-5}$

Figure 2.7 Safety Integrity Level (SIL) and according dangerous Probability of Failure per Hour (PFH_D)

An informative annex in IEC 62061 provides a qualitative approach to do risk estimation and SIL assignment which can be used for an SRCF. Since this is informative, other approaches

may be used based on SIL assignment approach in IEC 61508-5. Risk estimation is done by estimating the following risk parameters for each hazard:

- Severity of harm Se
- Probability of occurrence of that harm as a function of the following items:
  - Frequency and duration of the exposure of persons to the hazard Fr
  - Probability of occurrence of a hazardous event Pr
  - Possibility to avoid or limit the harm Av

Severity of injury (Se) or damage to health is classified to have four levels:

1: is used to indicate a minor injury such as scratches and minor bruises that require attention by first aid

2: is used for reversible injuries, including severe lacerations, stabbing, and severe bruises that require attention from a medical practitioner

3: is used for major irreversible injury in such a way that it can be possible to continue the same work after healing

4: used for significant irreversible injury or death

Then each of other three parameters are estimated independently of each other. It is suggested that worst case scenario should be applied to avoid underestimation of any risk parameter.

Frequency and duration of exposure (Fr)	
Frequency of exposure	**Frequency, Fr** (see A.2.4.1)
≤ 1 per h	5
< 1 per h to ≥ 1 per day	5
< 1 per day to ≥ 1 per 2 weeks	4
< 1 per 2 weeks to ≥ 1 per year	3
< 1 per year	2

(a) Frequency and duration of exposure

Probability of occurrence	Probability (Pr)
Very high	5
Likely	4
Possible	3
Rarely	2
Negligible	1

(b) Probability of occurrence of a hazardous event

Probabilities of avoiding or limiting harm (AV)	
Impossible	5
Rarely	3
Probable	1

(c) Probability of avoiding or limiting harm

Figure 2.8 Parameters of probability of occurrence of harm

To define the level of exposure, the following aspects should be considered very carefully:

– Is there any need to access to the danger zone? On which modes of operation? (normal operation/maintenance/etc.)
– How many hours a day/week/month is the machine active and in use?
– What is the nature of access?

After determination of these aspects, an average interval between exposures is estimated. Additionally, the duration of exposure should be estimated based on these factors.

Another factor that should be determined is the probability of harm, which is estimated independently of the other factors. This parameter is estimated by considering the predictability of the behavior of components related to the hazard, and characteristics of human behavior who interacts with hazardous part. The standard suggests that “very high” has to be taken for normal operation and choosing any lower value requires specific reasons.

And the last parameter, probability of avoiding harm, is determined by taking into account speed of appearance of the hazardous event, spatial possibility to withdraw from the hazard, the nature of component or system (electrical hazard, sharpness, temperature, etc) and possibility of recognition of a hazard.

Comparing to graphical method in ISO 13849, using more precise definition for each level assures that expert can choose a more appropriate level for each risk parameter. These parameters are then used to find Cl from the following formula:

$Cl = Fr + Pr + Av$

Using the matrix SIL allocation in Figure 2.9 then a safety integrity level can be allocated to the safety function.

Severity (Se)	Class (Cl)				
	4	5-7	8-10	11-13	14-15
4	SIL 2	SIL 2	SIL 2	SIL 3	SIL 3
3		(OM)	SIL 1	SIL 2	SIL 3
2			(OM)	SIL 1	SIL 2
1				(OM)	SIL 1

Figure 2.9 Matrix method to estimate the safety integrity level (SIL) [3]

Although SIL assignment seems more promising than PL assignment, it has still limitations. Expert's opinion is the key source of information. Additionally, IEC 62061 is only valid for electrical and electronic safety functions and for other types of systems ISO 13849 has to be used. This requires that results from risk assessment in ISO 13849 and IEC 62061 be in accordance with each other. However, studies show that discrepancies exist in their results.

IEC 62061 mentions that in many machine specific standards, known as type C standard in CEN, risk estimation is carried out to find Category based on ISO 13849-1:1999 for safety related control functions. As such, for simplification, the relationship in Figure 2.10 between SIL and PL is suggested. Based on this relationship,PL b and c correspond to SIL 1, PL d correspond to SIL 2 and **PL e** corresponds to SIL 3. It also mentions that a better relation is under study. Is the relationship given in Figure 2.10 always valid?

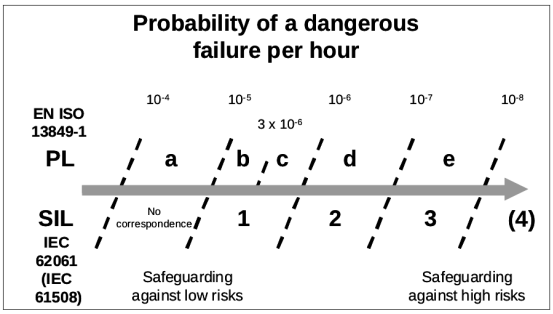


Figure 2.10 Safety Integrity Levels and their related Performance Level values (taken from [1])

Martiko et al. [4] have shown that results from risk level allocation using methods in the two standards may be different. They divided safety engineers into three groups and asked them to do risk assessment on a machine using safety definition and design methods of ISO 13849 and IEC 62061. The following interesting points are important to be mentioned:

– Safey level allocation done by different individuals may have different results.
– Results from risk allocation based on ISO 13849 (PL) may be different from the ones based on IEC 62061 (SIL).
– Results are mostly deviated toward the safe side.

Figure 2.11 shows results of this case study. As it can be seen, results from SIL assignment do not match with the ones from PL in all cases. To see this, we assign SIL to a safety function. Suppose that the severity of the accident caused by the hazard is not high, but may result to an injury, such that based on Figure 2.9, it is equal to level 2. Looking at the figure, we can see that with this severity level, SIL can be equal to one or two. Based on probability of dangerous failure per hour (look at Figure 2.10), SIL 2 is equal to PL d. However, if we look at performance level from ISO 13849, Figure 2.3, we can see that with low severity which is equal to S1, the performance level can not go higher than level c, which is equal to SIL 1. Thus, with the same severity level, one can conclude that the machine is at SIL=2 or SIL=1 (PL=c).

Table 6
Results of the risk estimation for a control function of the system under study achieved in Case study 1.

Group no.	Case study 1																			
	Risk estimation based on IEC 62061												Risk estimation based on ISO 13849-1							
	Se		Fr		Pr		Av		PL		SIL		*S*		*F*		*P*		PL	
	Ex. 1	**Ex. 2**	Ex. 1	**Ex. 2**	Ex. 1	**Ex. 2**	Ex. 1	**Ex. 2**	Ex. 1	**Ex. 2**	Ex. 1	**Ex. 2**	Ex. 1	**Ex. 2**	Ex. 1	**Ex. 2**	Ex. 1	**Ex. 2**	Ex. 1	**Ex. 2**
1	2	**3**	3	**3**	2	**2**	1	**1**	–	**a**	–	**–**	1	**na**	1	**na**	1	**na**	a	**na**
2	3	**3**	5	**5**	2	**3**	3	**1**	c	**c**	SIL 1	**SIL 1**	na	**na**	na	**na**	na	**na**	na	**na**
3	4	**4**	3	**3**	4	**4**	3	**3**	d	**d**	SIL 2	**SIL 2**	2	**na**	1	**na**	1	**na**	c	**na**
4	3	**3**	5	**3**	2	**2**	1	**3**	b	**b**	SIL 1	**SIL 1**	2	**2**	1	**1**	1	**1**	c	**c**
5	4	**4**	5	**5**	2	**2**	3	**3**	d	**d**	SIL 2	**SIL 2**	2	**na**	2	**na**	1	**na**	d	**na**
6	4	**3**	4	**3**	3	**2**	3	**3**	d	**b**	SIL 2	**SIL 1**	2	**1**	1	**1**	1	**1**	c	**a**
7	4	**4**	5	**5**	2	**2**	3	**3**	d	**d**	SIL 2	**SIL 2**	2	**2**	2	**2**	1	**2**	d	**e**
8	4	**4**	3	**3**	3	**3**	3	**3**	d	**d**	SIL 2	**SIL 2**	2	**2**	1	**1**	2	**2**	d	**d**
9	3	**3**	3	**3**	3	**3**	3	**3**	c	**c**	SIL 1	**SIL 1**	2	**2**	1	**1**	1	**1**	c	**c**
Average	3.4	**3.4**	4.0	**3.7**	2.6	**2.6**	2.6	**2.6**	3.1	**3.0**	1.4	**1.3**	1.9	**1.8**	1.3	**1.2**	1.1	**1.4**	3.1	**3.2**
St. dev.	0.7	**0.5**	1.0	**1.0**	0.7	**0.7**	0.9	**0.9**	1.4	**1.1**	0.7	**0.7**	0.4	**0.4**	0.5	**0.4**	0.4	**0.5**	1.0	**1.5**

Table 7
Results of the risk estimation for a control function of the system under study achieved in Case study 2.

Group no.	Case study 2																	
	Risk estimation based on IEC 62061										Risk estimation based on ISO 13849-1							
	Se		Fr		Pr		Av		SIL		*S*		*F*		*P*		PL	
	Ex. 1	**Ex. 2**	Ex. 1	**Ex. 2**	Ex. 1	**Ex. 2**	Ex. 1	**Ex. 2**	Ex. 1	**Ex. 2**	Ex. 1	**Ex. 2**	Ex. 1	**Ex. 2**	Ex. 1	**Ex. 2**	Ex. 1	**Ex. 2**
1	4	**4**	5	**5**	3	**3**	3	**3**	SIL 3	**SIL 3**	2	**2**	2	**2**	1	**1**	d	**d**
2	4	**na**	5	**na**	3	**na**	3	**na**	SIL 3	**na**	2	**na**	2	**na**	1	**na**	d	**na**
3	4	**4**	4	**4**	2	**2**	3	**3**	SIL 2	**SIL 2**	2	**na**	2	**na**	2	**na**	e	**na**
4	3	**4**	5	**2**	2	**2**	3	**3**	SIL 1	**SIL 2**	2	**2**	1	**1**	2	**2**	d	**d**
5	4	**4**	4	**4**	3	**3**	3	**5**	SIL 2	**SIL 3**	2	**2**	1	**1**	2	**2**	d	**d**
6	4	**4**	5	**5**	3	**3**	3	**3**	SIL 3	**SIL 3**	2	**2**	2	**2**	2	**2**	e	**e**
7	4	**4**	3	**3**	3	**3**	3	**3**	SIL 2	**SIL 2**	2	**2**	1	**1**	2	**2**	d	**d**
8	4	**4**	2	**3**	2	**5**	5	**3**	SIL 2	**SIL 3**	2	**na**	2	**na**	1	**na**	d	**na**
9	4	**4**	4	**5**	3	**3**	3	**3**	SIL 2	**SIL 3**	2	**2**	2	**2**	1	**1**	d	**d**
Average	3.9	**4.0**	4.1	**3.9**	2.7	**3.0**	3.2	**3.3**	2.2	**2.6**	2	**2**	1.7	**1.5**	1.6	**1.7**	4.2	**4.2**
St. dev.	0.3	**0.0**	1.1	**1.1**	0.5	**0.9**	0.7	**0.7**	0.7	**0.5**	0	**0**	0.5	**0.5**	0.5	**0.5**	0.4	**0.4**

Figure 2.11 Case study done by Martiko et al. [4]; they have grouped engineers in different groups to study how they do risk allocation based on methods ISO13849 and IEC62061

Another way to show that results between PL and SIL can be different is shown in Figure 2.12. As an example in allocating SIL if severity is equal to three, for different values of Cl, SIL varies from below one to three which are equal ro PL=b to PL=e. According to relationship between SIL and PL, SIL=1 is equal to PL=b or c and SIL =3 is equal to PL e. However, based on definitions given for severity in ISO 13849 and IEC 62061, severity of 3 in SIL allocation can be related to S2 in PL allocation. This means that for severity level of S2 in graphical risk assessment PL can vary from PL=c to e and consequently results from two risk allocation do not match.

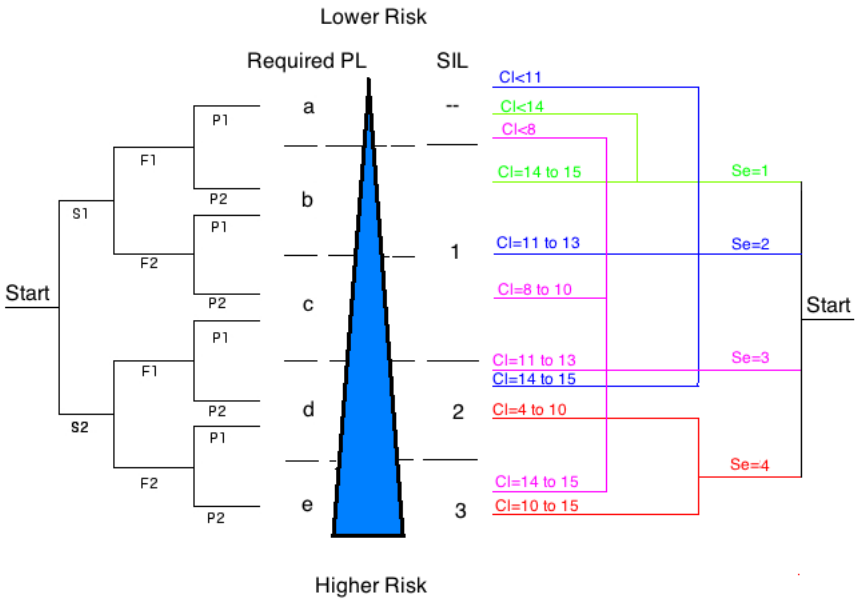


Figure 2.12 The relationship between PL and SIL. From right: PL allocation, from left: SIL estimation.

One way to solve this problem, is to use fuzzy and possibility theory. By using possibility theory, not only expert can present his opinion on a risk as a value between two risk levels in ISO 13849, (s)he is able to present it as a function. This way he can indicate which values of risk parameter are more probable.

This method can solve two problems related to risk allocation in safety standards to some extent. One problem is the inconsistency between the allocation results. It can be solved by presenting fuzzy values instead of crisp levels, which represent membership degree to each risk level. For example, in graphical risk allocation in ISO 13849, severity can have a fuzzy value between S1 and S2 which represent degree of membership to each of these two levels. As such, if severity in Matrix risk allocation of IEC 62061 is equal to 3, a fuzzy value in that range can be allocated to severity in graphical allocation (see Figure 2.13). To make results more **consistent**, risk level definitions from IEC 62061 can be used such that, instead of reversible and irreversible, four levels from matrix allocation are used.

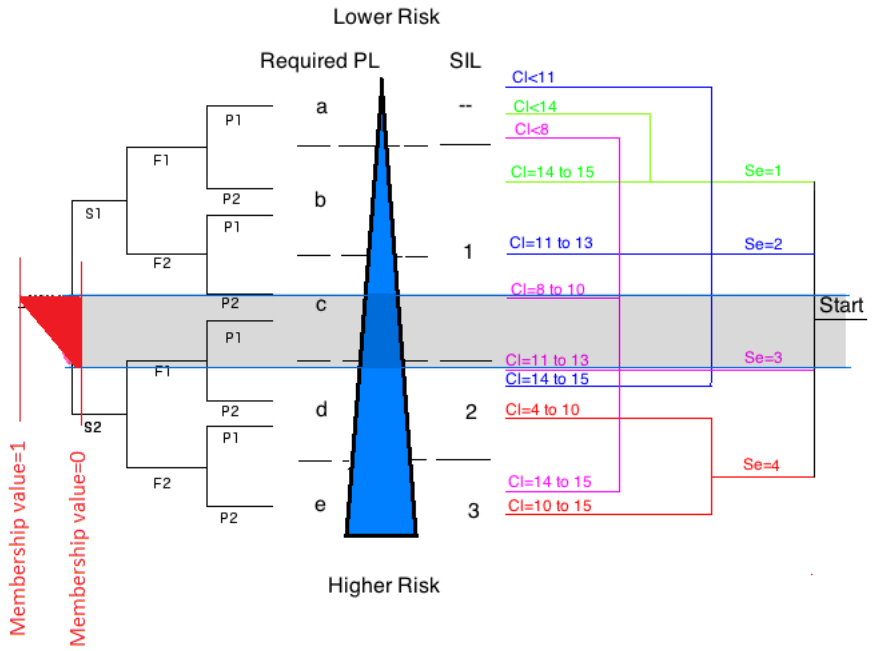


Figure 2.13 Using fuzzy to solve inconsistency between Severity parameter

Another problem with risk allocation is using expert's opinion. Using expert opinion is always prone to error. It has been shown that using possibility theory can improve the results by improving the subjectivity that exist in human opinion.

The objective of second paper is to propose a new methodology based on possibility theory to improve risk allocation methods already in use in safety standards, ISO 13849 and IEC 62061, such that their result match and it solves the problem of inconsistency between their results. Improving risk allocation and verification in ISO 13849 based on risk factor definition in IEC 62061, not only improves pulling opinion from experts, it also minimizes discrepancy between risk allocation and safety level verification of the two standards.

2.2 Literature review

Introduction of standards on safety related control systems that use probabilistic methods was a breakthrough in improving safety control systems. Since then, people have tried to introduce these standards and improve the way they are used in industry [19, 20, 21]. Not only

such studies have made a brighter view for designers to use standards, some also highlighted interesting practical and theoretical problems that exist in using standards. Institute for Occupational Safety and Health (IFA) in Germany, has published a report on using ISO 13849 to design safety control systems [1]. This report can be viewed as a reference in using ISO 13849. It has detailed explanation of each step to be followed, and at the end it provides various design examples already done at IFA. Another example for using ISO 13849 is provided in [20] and each step is described in detail. Confusion in using standards is discussed in [22]. It highlights the overlap between the two standards and then differences by considering safety levels. It explains similarities and differences in scope and level of complexity. Fukuda et al. [23] have shown that the simplified method to find performance level in ISO 13849 does not always give the same result as reliability analysis methods such as FTA [23]. Five circuits within different categories have been studied and results from fault tree analysis (FTA) and ISO 13849-1 are compared.

A fundamental step in applying a safety standard is doing risk level allocation. IFA has produced a computer-based tool to help users to find performance level [24]. Gauthier et. al. [25] compared risk assessment methods used in standard on safety related control systems; they used ISO/FDIS 14121-1 [12] as a benchmark. They showed that a level of variability in using safety assessment methods of these two standards exist. Their study showed that although risk assessment methods used in safety standards are fundamentally the same, but they exhibit significant differences which can make confusion for users. This is also highlighted in an article by Hietikko et al. [4]. They used risk assessment results from three case studies in machine safety and compared them with an expected risk assessment done by an expert. Their studies showed that people have difficulty in choosing right risk factors.

Risk allocation methods require evaluation from skilled experts. Experts are asked to evaluate risk parameters using descriptions provided for each risk factor. Using expert judgment is an essential source of information especially when no objective data is available. Since the nature of human judgment is inherently subjective and complex, elicitation of useful information requires a formal methodology. It was not until Cook and Goosens [26], who introduced a comprehensive and systematic methodology for treating expert judgment, that various methods have been proposed to pool, assess and combine experts' opinion. These methods are divided into two major groups: behavioral and mathematical approaches. Mathematical methods have shown better results than behavioral approaches [27]. Transferable belief model (TBM), based on Dempster-Schafer theory of evidence [28], has been employed in various fields such as: to find probability distribution in reliability [29], and in environmental studies [30]. TBM is a heuristic to model and evaluate objective and subjective evidence

to support a hypothesis. However, due to some restrictions of Dempster-Shafer theorem, this method may show limitations in safety analysis [31]. Probabilistic methods are also used to estimate reliability data [32], and do risk assessment [26]. Bayesian probabilistic approaches are broadly used in data-fusion. Despite interesting results they have shown in elicitation of human judgment, they require multiple sources of data, and are useful when used in human-sensor data fusion approaches.

Fuzzy systems have recently been used to deal with imprecision and uncertainty in reliability and safety analysis [33, 34, 35]. Nait-Said et. al. [36] proposed a fuzzy rule-based approach to improve conventional risk graph method used in IEC 61508. They showed how linguistic values in fuzzy can improve graphical risk assessment. They also provided a calibration method to design fuzzy scales. Sandri and Dubois [16] showed how fuzzy can be used to better educe expert opinion. They used possibility theory to deal with imprecision in expert judgment. Although possibility theory has been used in risk allocation method, it has never been used to address inconsistency problem that exist between two standards.

CHAPTER 3

CONTRIBUTION OF EACH PAPER

3.1 An Improvement in Applying Safety Standard "ISO 13849" Using Fuzzy Logic, SIAS 2012

Allocating PFH_d to safety function instead of performance levels, which are crisp values, can further be used in validation step to decrease the probability of over/under design. Conventional method in ISO 13849 requires transferring $MTTF_d$ and DC_{avg} values to crisp levels in order to find attained PL. In transferring non-crisp values to crisp levels, ISO 13849 rounds values toward the safe side which increases the probability of over-design. However, this paper suggests to use fuzzy risk allocation and validation which use PFH directly without transferring results to PLs that is required by conventional method.

Using fuzzy logic toolbox in Matlab, risk allocation method in ISO13849 is implemented. The risk allocation method in ISO 13849 uses risk parameters which have two levels. Therefore, only two linguistic membership values are used for each risk parameter. By using fuzzy set theory, experts can allocate values to risk parameters between zero and one to show risk estimation between low and high. To avoid unnecessary complexity, it is tried to use a simple model. Thus, semi-triangle functions are used for each membership function.

Figure 3.1 illustrates how membership values are determined based on fuzzy risk parameters. Since membership functions are chosen to be linear, this makes the fuzzy system easier to apply and understand. Expert opinion, presented as a value between zero and one, is translated into two membership values for each risk parameter. He is able to choose values for risk parameters (severity, frequency and possibility) between zero and one, which is not possible in crisp allocation.

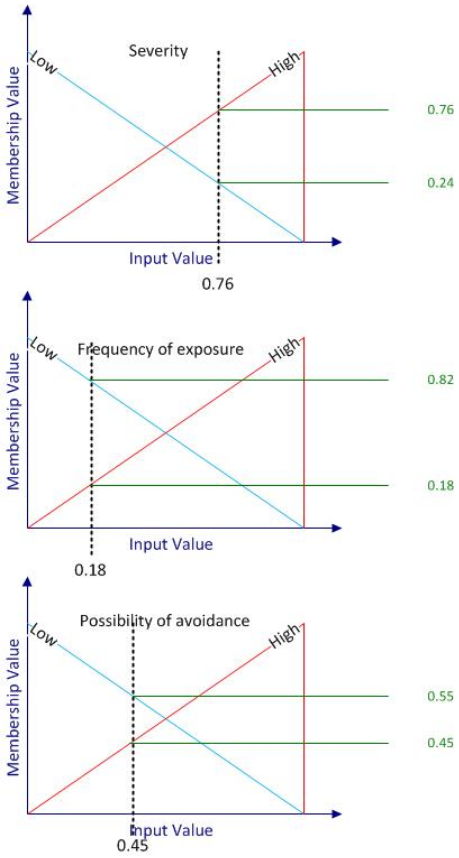


Figure 3.1 An example of choosing fuzzy risk parameter; choosing severity value of 0.76 means membership value of 0.76 for high severity and membership of 0.24 to low severity

As fuzzy inference system is applied, information flows through each step in the fuzzy system. The fuzzification-inference-defuzzification process generates a defuzzified output from an expert opinion. For any combination of risk parameters, the output shows required safety level as PFH. The result could be evaluated as PL by using max function for output membership functions, before defuzzification is performed.

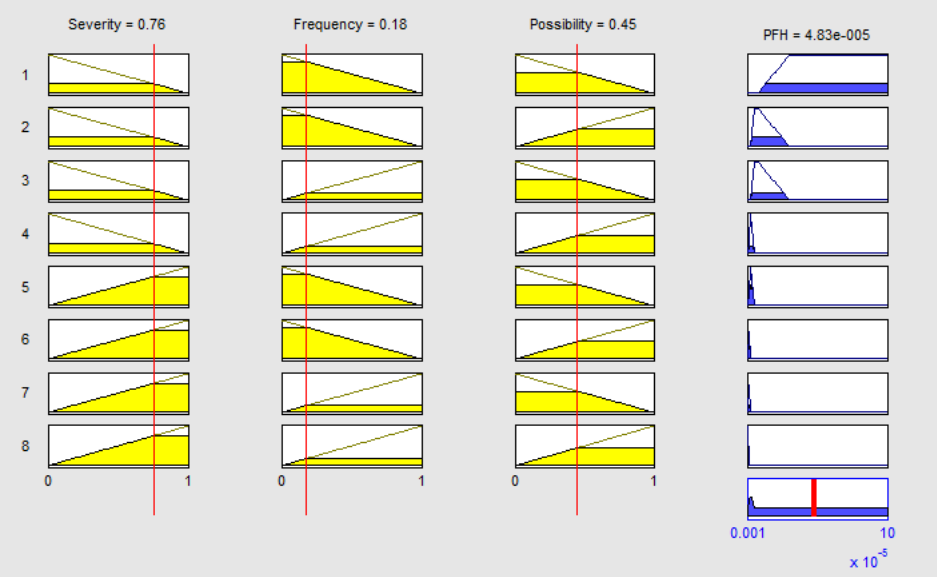


Figure 3.2 Matlab implementation of fuzzy risk allocation

Subsequent to design of a safety control system, achieved performance level (PL) has to be measured against $MTTF_d$ and DC_{avg}. These two measurements define the maximum claimable PL. The quality of analyses employed to validate an $SRCS$ in ISO 13848 and IEC 62061 is extremely important to assure reaching required safety. Such analyses are based on crisp levels where (PL), ($MTTF_d$) and (DC_{avg}) are calculated and defined with sharp boundaries. The variability of the failure rates to define $MTTF_d$ and DC_{avg} and also assumptions used in the standard for analytical models are based on uncertain and subjective nature of information applied.

At the evaluation step, the result is interesting. Table [4] in the paper shows the result of crisp evaluation against fuzzy evaluation technique. For values near transition points in Table 1 and 2, conventional approach is very sensitive to changes. The difference between 89.9% and 90.1% can result to a change in PL regardless of MTTFd value. This is due to the fact that transitions are crisp, and no difference is given to MTTFd and DCavg unless there is a change in their level.

3.2 Fuzzy Performance Level Allocation in Machine Safety Standards

Using fuzzy set theory two major problems in using the two safety standards, ISO 13849 and IEC 62061, can be solved to some extent. First problem in using these standards is different approaches they use to define required and achieved safety level for safety related

control systems and second problem is presenting vagueness that exist in human opinion. ISO 13849 uses performance levels (PLs) and IEC 62061 uses safety integrity levels (SILs). Although safety levels in both parameters are based on probability of dangerous failure per hour, methodologies used to define levels are different.

They differ in many aspects such as: deploying different number of risk parameters, levels in each risk parameter, definition of such levels, etc. However, relationship between PL allocation in ISO 13849 and SIL assignment in IEC 62061 suggests that required SIL and PL for a safety function have to be equal with respect to PFH, regardless of which safety standard is used. In other words, using table provided in both standards to transfer results between PL and SIL should give the same result as using PL and SIL allocation independently. However, it can be shown that in practice, relationship in Table 1 does not hold for some cases. The following points can be mentioned as reasons:

1) Number of risk parameters are different

First difference between safety allocation methods is in number of risk parameters used in each standard. The matrix SIL assignment method uses four risk parameters while graphical PL allocation uses three risk parameters. In fact, probability of occurrence is not considered in PL allocation method. Thus, it can be said that PL allocation method does not distinct between probable and rare situations. According to IEC 62061, influential parameters to estimate the probability of occurrence of hazard are machines conduct in different modes of operation and human interaction with the machine.

2) Number of levels for each parameter

Another difference between two methods is in number of levels determined for each risk parameter. Risk parameters in ISO 13849 have two levels, while in IEC 62061, 3 to 5 levels are used for each risk parameter. Increasing levels for parameter enables experts to associate detailed description to a hazard, however, it also increases the complexity.

Reassigning linguistic values based on fuzzy sets used in defining levels in risk parameters, can help to design an allocation method which its result is more comparable to both approaches. This way, safety level from new fuzzy method may be used by both safety standards and ultimately solves the problem of discrepancy between results from two methods. Advantage of fuzzy approach is that the new method is in accordance with both standards. Fuzzy method used in this paper to transfer information from experts to a mathematical model, which then is used to define safety levels, is a solution to solve elicitation problem.

The contribution of this paper is to propose a risk allocation method using possibility theory

to solve two main problems in performance level allocation of safety standards ISO 13849 and IEC 62061:

– The subjectivity of using expert opinion to define risk parameters
– The inconsistency of risk allocation levels between methods in safety standards ISO 13849 and IEC 62061

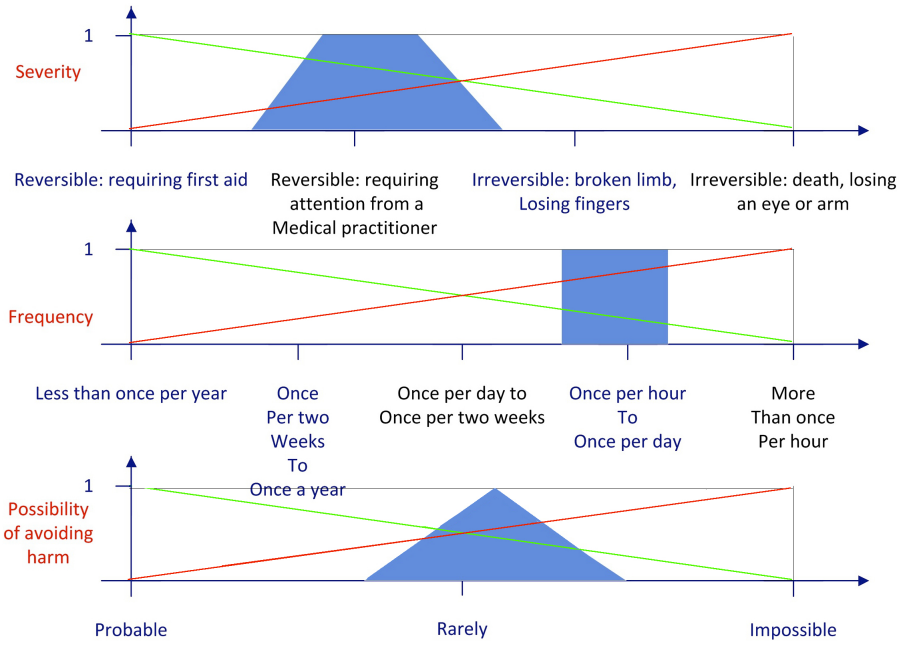


Figure 3.3 Using possibility theory to evaluate risk parameter

Another problem with conventional PL allocation is using vague expert's opinion. Possibility theory can deal effectively with such problem by using linguistic values and fuzzy ranking functions. Instead of transferring thought to single level, expert is capable to present his idea as a function, representing his vague opinion (see Figure 3.3). Three functions that may be used are: rectangle, triangle and trapezoid. Rectangle is used when expert wants to assign risk parameters to an interval, meaning that possibility of risk parameters to exist in this interval are the same. While using triangle, possibility of one point is more than others and end points of the triangle define interval that there is any possibility. By using trapezoid, expert first defines an interval which shows values that are possible (lower lateral) and then s(he) defines which values are most possible (upper lateral). The upper lateral is a way to show vagueness that can not be expressed in normal fuzzy systems.

Risk parameters in ISO 13849 are represented by fuzzy functions, while membership values of these fuzzy functions are defined based on risk parameters in IEC 62061. By using more

precise definitions of risk parameters in IEC 62061, not only defining the fuzzy function is more precise, but also problem of inconsistency between results would be minimized. Thus, what expert does is to transfer his opinion on risk graphical parameters of ISO 13849, based on risk definition of IEC 62061. Fuzzy functions are then fed into fuzzy inference system based on risk allocation rules of ISO 13849 to find required risk level.

One issue with using fuzzy logic is to set membership and de-fuzzification functions. Membership functions used in this approach have the simplest shape, linear between two possible end points while non-linear MFs such as sigmoidal can be considered. Defuzzification method may be discussed among experts to choose the most appropriate PL for a safety function. A method to set de-fuzzification function is to use neuro-fuzzy system. A set of safety functions with known PLs can be presented to the neural network that learns the nonlinear function and can then help to choose de-fuzzification function parameters by decreasing error between the results.

Another point to consider is the reliability of experts. This may be solved by presenting problems with known answers to experts and then using nonlinear functions to interpret their opinion. A tolerance level can also be set for acceptance of opinion. If opinion passes this level, the expert can be categorized as invalid and unreliable.

Using expert systems in critical decision making problems are more informative approaches rather than reliable final decision making approaches. The fuzzy approach can be an informative approach to help experts in allocating PL and SIL to a safety related control system. It can decrease the ambiguity of results form safety standards, especially when results are not in accordance. As mentioned, the result of using possibility theory can be discussed and help to improve choosing appropriate performance level.

CHAPTER 4

CONCLUSION

The intuitive concept of fuzzy logic is a way to show how real world is sensed and described by human. Fuzzy logic is actually a way to model systems using human reasoning approach. The result is that fuzzy can deal with ambiguities that exist in human driven measurements. Since risk allocation requires human reasoning to be used, fuzzy can help in this respect. Both papers try to illustrate the advantages of using fuzzy logic over conventional risk allocation methods.

First paper studies employing fuzzy in risk allocation and validation of risk level in ISO 13849. Using fuzzy in the risk allocation method step in both standards can improve the results. Transferring opinion about risk parameters is not appropriate in conventional methods, thus using a modeling method that can improve knowledge extraction from human is helpful. In this paper, triangle function as a simple membership function is used. Paper illustrates the performance of using fuzzy logic in risk allocation. This way, expert is able to choose values between high and low and show degree of membership for each risk parameter. For each risk paramter, two membership values enter fuzzy PL allocation inference system. The result of fuzzy PL allocation can be expressed in probability of failure per hour. Thus not only using fuzzy in risk allocation step can deal with transferring linguistic values into values, but also it can transfer the result into PFH_d. This paper also studies validation of designed control system versus required safety level. It is shown that fuzzy can deal with errors in data by transferring crisp levels into smooth levels. In conventional validation method, error in data can cause PL to be changed and result big errors. However, in fuzzy validation error is a continous nonlinear function of changes.

Using simple membership function was used for the sake of simplicity. However, other membership functions have to be studied. Another improvement is to design output fuzzy functions. Output fuzzy functions are used to transfer fuzzyfied values from inference system into PFH_d. This is done by allocating a transfer function to each performance level. In this paper, they were designed intuitively to show fuzzy advantages. Some approaches exist to improve these functions. One way is to use neuro-fuzzy. The idea is to have various designed safety functions already validated by other modelling approaches, and feed them into neural network while the output is knows. So neuro-fuzzy system tries to decrease error in the

output by changing functions.

The second paper extends the allocation method of first paper while trying to improve its results. By using fuzzy functions and possibility theory and then adapting the risk allocation method of ISO 13849 to IEC 62061, not only the risk allocation method is based on an improved pooling method, it is also more comparable to results from IEC 62061. This way, using each one of the safety standard should give the same required safety level.

To keep the analysis easy and show important aspects of using fuzzy in risk allocation and validation, the simplest form of membership function is used. Further analysis of other membership functions, such as sigmoidal function can reveal the power of dealing with human perception that exists in fuzzy. In fact, human perception uses nonlinear function to learn and perceive information from world around.

This paper does not consider elicitation of multiple experts which happens in real world. An improvement is to use elicitation methods that exist in fuzzy theory. Additionally, experts are considered to be at the same level of performance. Various approaches exist to consider experts with different level of performance. This way, reliability of experts can be studied further.

REFERENCES

[1] "Functional safety of machine controls (bgia report 2/2008 e)," tech. rep., Institute fur Arbeitsschutz der Deutschen Gesetzlichen Unfallversicherung, 2008.

[2] International Organization for Standardization, *ISO 13849-1:2006 - Safety of Machinery - Safety related parts of control systems - Part 1: General principles for design*, 2006.

[3] International Electrotechnical Commission, *Safety of Machinery - Functional Safety of Safety-Related Electrical, Electronic and Programmable Electronic Control Systems*, 1.0 ed., 2005.

[4] M. Heitikko., T. Malm, and J. Alanen, "Risk estimation studies in the context of a machine control function," *Reliability Engineering and System Safety*, vol. 96, pp. 767–774, July 2011.

[5] "National census of fatal occupational injuries in 2008," tech. rep., Statistics, Bureau of Labor, August 2009.

[6] European Commission, Enterprise and Industry, *Machinery Directive 2006/42/EC*, 2006.

[7] I. L. Organization, *Safety in Numbers*, 2003.

[8] L. R. and R. P., "Occupational injuries and diseases in canada, 1996-2005, injury rates and costs to the economy," *Human Resources and Social Development Canada*, May 2007. `http://www.hrsdc.gc.ca/en/labour/publications/health_safety/pdf/oidc.pdf`.

[9] B. M. Chambers C., Croll PR., "A study of incidents involving programmable electronic safety-related systems," *Interacting with computers*, vol. 11, pp. 597–609, June 1999.

[10] L. Giraud, "Machine safety - prevention of mechanical hazards - fixed guards and safety distances," Tech. Rep. RG-597, IRSST, 2009.

[11] F. Donateur, "Integrated safety in converters: Functional safety with modern ac drives," *echatroniK*, vol. 120, no. 5, pp. 20–21, 2012.

[12] International Organization for Standardization, *EN ISO 14121, Safety of machinery - Risk assessment*, 2007.

[13] International Organization for Standardization, *EN ISO 12100, Safety of machinery, General principles for design - Risk assessment and risk reduction*, 2010.

[14] *EN 954-1, Safety of machinery - Safety-related parts of control systems*, 1997.

[15] International Organization for Standardization, *ISO 13849-2:2003 - Safety of Machinery - Safety related parts of control systems - Part 2: Validation*, 2003.

[16] D. D. S. Sandri, "Elicitation, assessment and pooling of expert judgment using possibility theory," *IEEE Transaction on Fuzzy Systems*, vol. 3, pp. 313–335, August 1995.

[17] J. Y. Halpern, *Reasoning about uncertainty*. Cambridge: Mass: MIT Press, 2003.

[18] L. A. Zadeh, "Fuzzy sets," *Information and Control*, vol. 8, no. 3, pp. 338–353, 1965.

[19] E. Soressi, "Introduction in safety rules en954-1, en13849 and en62061," vol. V.2010, Issue 567, pp. 330–343, IET Conference Publications, 2010.

[20] 4th International Conference on Safety of Industrial Automated Systems, *EN ISO 13849: A practical standard to evaluate control system for safety*, Sept. 2005.

[21] 4th International Conference on Safety of Industrial Automated Systems, *IEC 62061: An oveview of its principles, methodologies and applications for functional safety of electrical, electronic and programmable electronic safety-related control systems at machinery*, sep 2005.

[22] R. Piggin, "What's happening with machine safety standards and networks?," *Assembly Automation*, vol. 26, no. 2, pp. 104–110, 2006.

[23] *Evaluation of operation reliability of safety related part of control system of machine and safety level*, (Japan), SICE, Sept. 2007.

[24] "Software-assistent sistema - safety integrity software tool for the evaluation of machine applications," November 2008.

[25] Y. C. Francois Gauthier, Serge Lambert and J. J. Paques, "A comparative analysis of risk assessment for industrial machines in standards on safety related control systems," pp. 46–51, 2007.

[26] L. G. R.M. Cooke, "Procedures guide for structured expert judgment in accident consequence modeling," *Radiation Protection and Dosimetry*, vol. 90, no. 3, pp. 303–309, 2000.

[27] F. Ouchi, "A literature review in the use of expert opinion in probabilistic risk analysis," *Technical Report 3201,*, 2004.

[28] G. Shafer, *A mathematical theory of evidence*. Princton University Press, 1976.

[29] P. Smets, "The transferable belief model for expert judgment and reliability problems," *Reliability engineering and Systems Safety*, vol. 38, no. 2, pp. 59–66, 1992.

[30] M. H. Duong, "Hierarchical fusion of expert opinions in the transferable belief model, application to climate sensitivity," *International Journal of Approximate Reasoning*, vol. 49, pp. 555–574, 2005.

[31] D. Gerts, *A transferable belief model representation for physical security of nuclear materials.* Idaho National Laboratory, 2010.

[32] N. S. S. Campodonico, "Inference and predictions from poisson point process incorporating expert knowledge," *Journal of the American Statistical Association*, vol. 90, no. 429, pp. 220–226, 1995.

[33] J. B. Bowles and C. E. Pelaez, "Fuzzy logic priotrization of failures in a system failure mode, effects and criticality analysis," *Reliability Engineering and System Safety*, vol. 50, no. 2, pp. 203–213, 1995.

[34] A. Pillay and J. Wang, "Modified failure mode and effects analysis using approximate reasoning," *Reliability Engineering and System Safety*, vol. 79, no. 1, pp. 69–85, 2003.

[35] M. M. A. S. Markowski and A. Bigoszewska, "Fuzzy logic for process safety analysis," *Proceedings of the International Symposium of Process Safety Center*, October 2007.

[36] F. Z. R. Nait-Said and N. Ouzraouni, "Fuzzy risk graph model for determining safety integrity level," *International Journal of Quality, Statistics, and Reliability*, vol. 2008, p. 12, 2008.

ANNEXE A

AN IMPROVEMENT IN APPLYING SAFETY STANDARD "ISO 13849" USING FUZZY LOGIC, SIAS 2012 (Published)

SIAS 2012

An Improvement in Applying Safety Standard "ISO 13849" using Fuzzy Logic

Mohammad Sohani, Yuvin Chinniah, Mohamed-Salah Ouali

KEYWORDS:

ABSTRACT

Accurate risk allocation and validation steps are essential to apply ISO 13849 standard on safety related control systems. However, failure rate data is rarely available to designers and usually not provided with components used in safety systems. Recently, manufacturers have started to perform measurements for failure rates in order to include them into their data sheets. Meanwhile, other data sources may be used which encompass uncertainty and error due to dissimilar specifications between test and implementation environment. Conventional methods used in standards based on crisp levels are not appropriate in this respect. Additionally, risk assessment method employed to define required performance level (PL_r) for the safety control system uses expert's opinion to define risk component levels. Using expert's opinion entails subjectivity problem and crisp values are not appropriate to express judgmental risk assessment. Applying fuzzy logic in the standard can solve both these problems. Fuzzy logic has been proven to deal effectively with uncertainty and subjectivity. It can improve the methodology and reduce under or overdesign possibility.

1 INTRODUCTION

The aim of performing risk reduction on an industrial machine is to satisfy requirements of safety regulations and standards and also to ensure sufficient safety. Acceptable risk for a machine is achieved by using a combination of methods including intrinsic safe design, safeguarding and training. Accordingly, functional safety can be used as an effective and useful approach in reducing associated risks linked to machine. Functional safety is "part of the safety of the machine and the machine control system which depends on the correct functioning of the SRECS, other technology safety-related systems and external risk reduction facilities" [1]. When used for industrial machine, it is realized by deploying safety related control (SRC). To design SRC, standard ISO 13849 [2] is required to guarantee required safety level. This standard uses performance levels (PLs), each associated with an interval of probability of failure per hour (PFH), to classify safety related control systems based on their resistance to faults. These levels show how much SRC system should contribute in the risk reduction process and show their safety level. The method used in ISO 13849 requires performing risk assessment and associating a performance level to the safety control system. It uses graphical method and defines the required performance level as a combination of three parameters. Each risk parameter is found based on expert's opinion. Using expert's opinion to define risk parameters, however, is imprecise and uncertain [3]. Moreover, performance level allocations are frequently conservative as a result of accumulation of assumptions to be on the safe side. Furthermore, performance levels (PLs) are defined as crisp intervals and crisp intervals are not appropriate especially when PFH is marginally in an interval. Another type of uncertainty encountered is related to the lack of knowledge about the machine and vagueness in interpretation of risk components. The designed safety control system is then validated against requirements of the associated performance level.

The quality of analyses employed to validate an SRCS is extremely important to assure safety. Such analyses are based on crisp levels where performance level (PL), mean time to dangerous failure ($MTTF_d$) and average diagnostic coverage (DC_{avg}) are calculated and defined with sharp boundaries. The variability of the failure rates to define $MTTF_d$ and DC_{avg} and also assumptions used in the standard for analytical models are based on uncertain and subjective nature of information applied. It is difficult to collect failure rate data for all components and in many cases companies do not provide such data with their components. In such cases, external sources such as MIL-HDBK-217F, IEC/TR 62380, NPRD 95 or IEC 61709 have to be used which entail imprecise information.

As a conclusion, resulting safety function may be considered inexact and the outcome could be an under or over-designed function. An under-design can be dangerous since no adequate risk reduction is obtained. An over design can also be a problem since the additional cost can be a deterrent to the implementation of such measures. Thus, it is important to look for methods that can deal with imprecision in reliability data and subjectivity of risk assessment method. An approach can be using fuzzy logic [4], [5]. Fuzzy has been recently applied successfully in reliability and safety field [6-8]. Nait-Said et al. [9] used fuzzy to solve inconsistency problem in the result of graphical risk

assessment method, caused from subjectivity and interpretation problem. They showed how linguistic values in fuzzy can improve graphical risk assessment. They also provided a calibration method to design fuzzy scales. Sandri and Dubois [3] showed how fuzzy can be used to better educe expert's opinion. They used possibility theory to deal with imprecision in expert judgment.
The contribution of this paper is to use fuzzy logic to improve methodology of ISO 13849 and help defining requirements of the safety control function. It will be shown how the risk of under/over design, which entails expensive system, can be decreased. This paper is structured as follows. Section 2 discusses the required steps in ISO 13849 to design a SRC and existing shortcomings. Section 3 states the fuzzy approach, and Section 4 provides results from an example.

2 ISO 13849

In 1999, ISO published a new standard using probabilistic methods in addition to previous qualitative measurements in EN 954. To mitigate the pain of using probabilities and various quantifiable measurements, the standard introduced a simpler approach using graphical tools and designated structures [2]. Although using probabilistic approach is a breakthrough in designing safety systems for industrial machines, there are still shortcomings in using such methods.
After studying the machine and its limitations, required safety functions to secure the machine can be identified. Consequently, if safety function has to be implemented using a SRC system, a detailed specification has to be provided for each SRC. A required performance level is then allocated to SRC by using simplified graphical allocation method (See Figure 1).

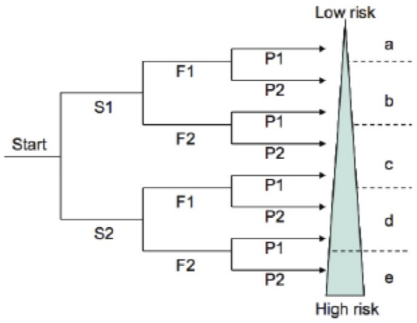


Figure 1. Determination of Performance Level (PL) based on Severity of injury (S1: reversible injury,S2: irreversible and death), Frequency and/or exposure to hazard (F1: low, F2: high), Possibility of avoiding hazard or limiting harm (P1: possible under specific conditions, P2: scarcely possible).

Three risk parameters, namely: severity of injury (S), frequency and exposure to hazard (F), and possibility of avoiding hazard or limiting harm (P) have to be determined. For each parameter two levels are defined. These parameters are then translated to PLs as illustrated in Figure 1. These are lingual values associating a situation to one of the five PLs. One or more experts are asked to give their opinion about each parameter by choosing between linguistic values. Such pooling method is prune to error due to subjectivity and having crisp levels [3].
Subsequently, each PL is associated with a design structure for input, logic and output. After the design is finished, SRC has to be assessed against various performance criteria to verify if required performance level is attained. The three quantitative measurements used in ISO 13849 are: mean time to dangerous failure ($MTTF_d$), average diagnostic coverage (DC_{avg}). Since performance levels as well as $MTTF_d$, DC_{avg} are defined as crisp intervals, for a wide range of probabilities it is probable to under/over design the safety function. Next section shows how fuzzy system is defined and can improve the result.

3 Fuzzy Logic

Fuzzy sets constitute one of the most influential notions in engineering and science. The concept of fuzzy set is intuitive and transparent as it defines how the real world is perceived and described by human. Fuzzy logic has been proven to be a powerful tool to model nonlinear, complex and ill-defined systems [10]. Unlike conventional modeling tools, it is based on human reasoning capability in complex and imprecise environment. Consequently, in

contrast to approaches that require accurate equations to model real world systems, fuzzy logic can deal with existing ambiguities in human driven measurements and judgments.
A membership value $\mu_A(x)$ is allocated to each value of x in the fuzzy set A. The membership value shows grade to which an element x belongs to the fuzzy set A. The power of fuzzy is originated from the fact that an element can simultaneously belong in degrees to two fuzzy sets. Various functions, called fuzzifiers, can be deployed as membership functions. However, trapezoid and triangular functions are the most common fuzzifiers. Choosing the type of the membership function depends on the context and generally is arbitrarily according to the user experience [11].

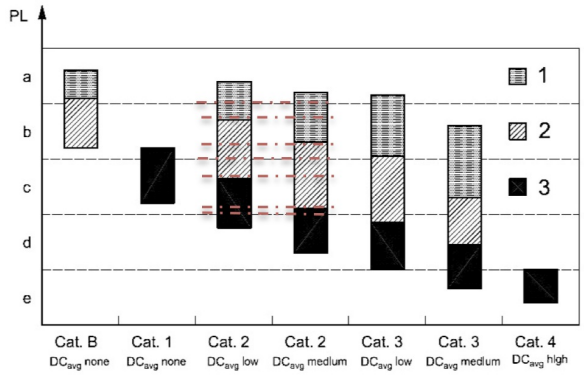


Figure 2. Simplified method to verify PL attain from using the SRC. 1: Low MTTFd, 2: Medium MTTFd, 3: High MTTFd (see Table 1 and 2).

Denotation of each channel	*MTTFd*
Low	3 years ≤ MTTFd < 10 years
Medium	10 years ≤ MTTFd < 30 years
High	30 years ≤ MTTFd ≤ 100 years

Table 1. Mean time to dangerous failure of each channel (MTTFd)

Notation	*DC*
None	DC < 60%
Low	60% ≤ DC < 90%
Medium	90% ≤ DC < 99%
High	99% ≤ DC

Table 2. Performance Levels and associated probabilities of dangerous failure per hour

Inputs are mapped to output membership function by passing through fuzzy logic inference system. Two popular fuzzy inference methods are Mamadani [12] and Sugeno (TSK). In TSK (Sugeno) model, rules are extracted from the input data. Although TSK-Sugeno is more powerful in modeling a system from data sets, the generated rules have no meaning for experts. In fact, Mamdani fuzzy type is more proper for generating models based on human reasoning and existing rules. Mamdani fuzzy inference has been successfully applied to various problems. The aggregation of fuzzy rules is a way to employ T-norms or T-conorms operators to combine multiple fuzzy sets and produce a single result. Any operator that has T-norm and T-conorm properties can be used, however, min-max operators that are used in this paper have the advantage of simplicity and have extensively been used.
In some cases, the results from fuzzy inference system (FIS) are required to be transformed into crisp numbers. This is in fact, the reverse of fuzzification process. Various approaches have been introduced for distinct applications, amongst which, the most extensively used approach is centroid-defuzzification.

A. Fuzzy determination of required Performance Level (allocation)

Making use of fuzzy logic toolbox in Matlab, the risk allocation method of Figure 1 is implemented. The universe of discourse for each risk factor is [0,1]. Since the risk parameters constitute two levels and it is essential to implement the assessment methodology of the standard, it is not possible to add linguistic values to risk parameters. Thus, only two linguistic membership values of: 'low' and 'high' are used. If X_1 means low and X_2 means high, then X is any risk factor used in the risk allocation method from the set (S, F, P); i.e S_1 means low severity or reversible injury while S_2 means high severity or irreversible injury. By using fuzzy set theory, experts can allocate values to risk parameters between zero and one to show risk estimation between low and high. Semi-triangle functions are used for each membership function (see Figure 3). For X_1, membership function is equal to one at zero, meaning that its membership value, $\mu_{X1}(x)$, is equal to one at zero and it decreases toward moving to one. The same theory holds for

X_2 at one and its membership grade decreases moving toward zero. Thus, moving from X_1 toward X_2 means decreasing membership of X_1 and increasing membership for X_2, i.e. moving from S_1 toward S_2 means increasing severity. Membership functions are defined as shown in Figure 3.

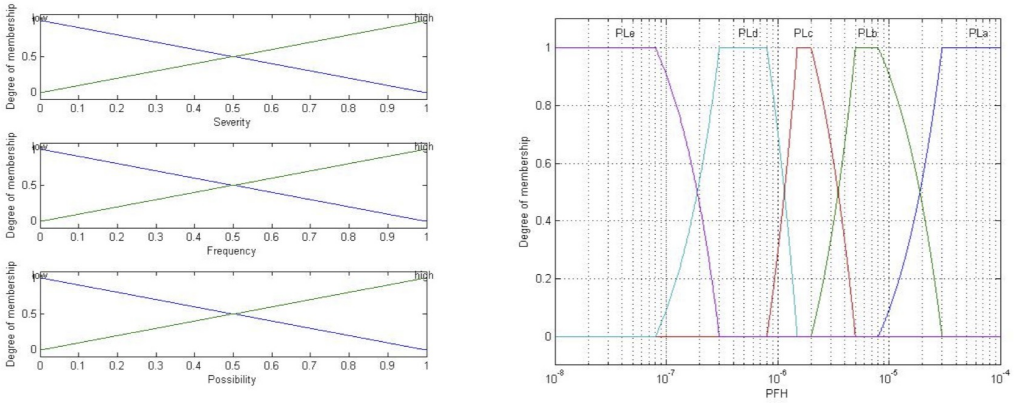


Figure 3. Fuzzification and de-fuzzification membership functions

Owing to the rules in the standard, the performance level determination method in Figure 1 is used to generate fuzzy rules. The total number of fuzzy rules is equal to eight. Table 3 shows rules generated based on risk allocation method in the standard.

	Severity		Frequency		Possibility		PL
1	S1	AND	F1	AND	P1	=>	a
2	S1	AND	F1	AND	P2	=>	b
3	S1	AND	F2	AND	P1	=>	b
4	S1	AND	F2	AND	P2	=>	c
5	S2	AND	F1	AND	P1	=>	c
6	S2	AND	F1	AND	P2	=>	d
7	S2	AND	F2	AND	P1	=>	d
8	S2	AND	F2	AND	P2	=>	e

Table 3. IF-THEN rules based on PLr allocation rules in the standard

The result of applying fuzzy rules is a set of values (a_1, a_2, a_3, a_4, a_5) showing degrees of each output membership performance level (PL_a, PL_b, PL_c, PL_d, PL_e). The last step is to defuzzify the membership values. Trapezoid membership functions are appropriate to transform linguistic values to PFH as they can represent a definite value in an interval. Membership degree of one is assigned to each function for intervals where values are definite, i.e. kernel of trapezoid. The difference between kernel and support (see Figure 5) depends on degree to which engineering and management group may accept a performance level to be part of a higher or lower PL. Strict PL allocation requires kernel to be equal to support, meaning that square membership function is used instead of trapezoid. Various defuzzification methods exist in the literature. Max function may be used when safe side results are required. The disadvantage of max function is that it considers one membership value. The centroid function, however, considers all membership function in the output.

B. Fuzzy validation of the implemented performance level

Subsequent to design of a safety control system, achieved performance level (PL) has to be measured against $MTTF_d$ and DC_{avg}. These two measurements define the maximum claimable PL.

Because category is defined based on the structure of SRCS, it has to be determined in advance and cannot be included in the fuzzy approach. Therefore, distinct fuzzy systems are designed for each category and the two variables $MTTF_d$ and DC_{avg} define maximum claimable PL. The membership functions are defined based on Tables 1 and 2 using trapezoid function.

Figure 4. Steps to design fuzzy validation

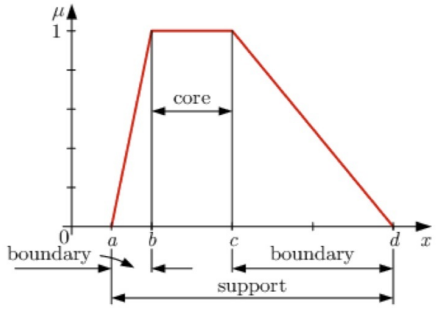


Figure 4. Trapezoidal membership function, distance between a and b = support, and distance between b and c = kernel

Minimum number of rules (n), required for each category depends on values of set S=(PL, $MTTF_d$, DC_{avg}). For each category, illustrated by squares in Figure 1, the following steps must be followed:

1. Minimum value of $MTTF_d$ in the category is chosen and n will be equal to 1.
2. Increase $MTTF_d$ and consider elements of set S.
3. If a level change occurs in any element of set S: increase n; end membership function for the element and start another membership function.
4. Go to step one and continue till end point of $MTTF_d$ in the category.

Membership functions are derived based on procedure above. Boundaries in trapezoid function give ability to a variable to be member of two neighbor sets.

4 Results and Conclusions

As explained in Section 3, as fuzzy inference system is applied, the information flows through each step in the fuzzy system. The fuzzification-inference-defuzzification process generates a defuzzified output from an expert opinion. For any combination of risk parameters, the output shows required safety level as PFH. The result could be evaluated as PL by using max function for output membership functions, before defuzzification is performed. If risk value cannot be shown as extreme values of 0 or 1, expert allocates his assessment by choosing a singleton value in between. A point in risk assessment, means expert is sure about the risk value. Figure 5 illustrates the fuzzy allocation. As it can be seen, expert is able to choose values for risk parameters (severity, frequency and possibility) between zero and one, which is not possible in crisp allocation.
Another evaluation technique is to use possibility theory to pool expert's opinion [3] and then rank each membership function by the expert judgment. Using possibility theory is not considered here.

At the evaluation step, the result is interesting. Table [4] shows the result of crisp evaluation against fuzzy evaluation technique. For values near transition points in Table 1 and 2, conventional approach is very sensitive to changes. The difference between 89.9% and 90.1% can result to a change in PL regardless of $MTTF_d$ value. This is due to the fact that transitions are crisp, and no difference is given to $MTTF_d$ and DC_{avg} unless there is a change in

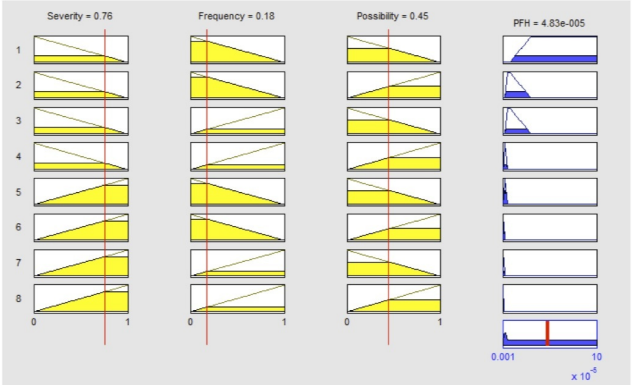


Figure 5. Fuzzy risk allocation; singleton evaluation of risk parameters

Item	$MTTF_d$	DC_{avg}	*PL: Conventional Approach*	*Fuzzy Approach*
1	6.8y: Low	80%	a	$1.21*10^{-5}$
2	6.8y: Low	89%	a	$9.98*10^{-6}$
3	6.8y: Low	91%	b	$9.83*10^{-6}$

Table 4. Validation based on conventional and fuzzy approach

their level.

5 References

1. *IEC 62061 ed1.0, Safety of machinery – Functional safety of safety related electrical, electronic and programmable electronic control systems*, International Electrotechnical Commission, 2005.
2. *ISO 13849-1, Safety of Machinery – Safety Related Parts of Control Systems – Part I, General Principles for Design,* International Standard Organization (ISO), 1999.
3. Sandri S., Dubois D., *Elicitation, Assessment and Pooling of Expert Judgments Using Possibility Theory*, IEEE Transaction on Fuzzy Systems, Vol. 3, No. 3, August 1995, pp. 313-335.
4. Wu Y., Zhang B., Lu J., Du K. L., *Fuzzy Logic and Neuro-Fuzzy Systems: A Systematic Introduction*, International Journal of Artificial Intelligence and Expert Systems (IJAE), Vol. 2, Issue 2, 2011.
5. Nait-Said R., Zidani F., Ouzraoui N., *Fuzzy Risk Graph Model for Determining Safety Integrity Level*, International Journal of Quality, Statistics, and Reliability, Vol. 2008.
6. Bowles, J. B., Pelaez C. E., *Fuzzy Logic Prioritization of Failure in a System Failure Mode, Effect and Critically Analysis,* Reliability Engineering and System Safety, 50, 1995, pp. 203-2013.
7. Xu K., Tang L. C., Xie M., Ho S. L., Zhu M. L., *Fuzzy Assessment of FMEA for Engine Systems,* Reliability Engineering and System Safety, 75, 2002, pp. 17-29.
8. Guimaraes A. C. F., Lapa C. M. F., *Fuzzy Inference to Risk Assessment on Nuclear Engineering Systems,* applied Soft Computing, 7, 2007, pp 17-28.
9. Nait-Said R., Zidani F., Ouzraoui N., *Modified Risk Graph Method Using Fuzzy Rule-Based approach,* Journal of Hazardous Materials, Vol. 164, 2009, 651-658.
10. Wang L., Langari R., *Complex Systems Modeling via Fuzzy Logic*, Proceedings of the 33rd IEEE Conference on Decision and Control, Vol. 4, 1994, pp. 4136-4141.
11. J. Mendel. Fuzzy logic systems for engineering: a tutorial. Proceedings of the IEEE, 83(3), pp. 345–377, Mar 1995
12. Mamdani E. H., *Application of Fuzzy Algorithms for Control of a Simple Dynamic Plant*, Proc. IEEE, 12(1), 1974, pp. 1585–1588.
13. http://www.mathworks.com/help/toolbox/fuzzy/trapmf.html

ANNEXE B

FUZZY PERFORMANCE LEVEL ALLOCATION IN MACHINE SAFETY STANDARDS (Submitted to the Journal of Reliability Engineering and System Safety)

Fuzzy Performance Level Allocation in Machine Safety Standards

Mohammad Sohani[1], Mohamed-Salah Ouali, Yuvin Chinniah[2]

Abstract*—Using fuzzy set theory, two major problems related to risk allocation in ISO 13849 and IEC 62061 safety standards on control systems, can be adequately solved. The first problem concerns the subjectivity of relying on expert opinion to define risk parameters, which are used to select the required level of safety for control systems. The second problem deals with the inconsistency of risk allocation levels between assessment methods in ISO 13849 and IEC 62061 standards. ISO 13849 uses performance levels (PLs) and IEC 62061 uses safety integrity levels (SILs) to characterize the machine's control system safety level. Although safety levels in both standards are based on probability of dangerous failure per hour, the methodologies used to define those levels are different. Reassigning linguistic values based on fuzzy sets, used in defining levels in risk parameters, can help to design an allocation method which has its results being more comparable to both approaches. This way, safety level from the proposed fuzzy method may be used by both safety standards and ultimately solves the problem of discrepancy between results from two methods. The advantage of fuzzy approach is that the proposed method is in accordance with both standards. Additionally, the use of expert's opinion, as the only source of information in defining safety level for a safety related control system is inherently subjective and complex. Therefore, elicitation of useful information requires a formal methodology. Fuzzy method is used in this paper to transfer information from experts to a mathematical model, which is then used to define safety levels. New fuzzy linguistic values are assigned for risk parameters based on IEC 62061, to find risk parameters in ISO 13849 and consequently required performance level. Instead of having a fuzzy value for each risk parameter, expert can express his opinion based on fuzzy function, using possibility theory. Such fuzzy functions can then fed to a fuzzy inference system (FIS) to find required PL. Theoretical background of method is presented and then the results are shown in a practical case study, using method on a plastic injection machine.

***Index Terms*—Safety Related Control Systems, ISO 13849, IEC 62061, Fuzzy Set Theory**

I. Introduction

Risk management is an iterative process that addresses reducing risks in industrial machines by using appropriate methods. Its ultimate target is to reduce the residual risk after design, by using a combination of technical and procedural safety methods such as protective guards, light curtain, safe working methods and training. Functional safety defined as, "part of the machine control system which depends on the correct functioning of the safety related control system and external risk reduction facilities" [3], has been proven to be an effective method to increase safety in industrial machines [34], [35]. Safety Related Electrical Control System (SRECS) is part of control system that realizes functional safety by responding appropriately to faults and errors. The quality requirements of SRECS for industrial machines are addressed in safety standards ISO 13849 [2] and IEC 62061 [3], while additionally, ISO 13849 comprises rules for non-electrical safety related control systems such as hydraulic and pneumatic. Both these standards define the framework to design SRECS required to reach adequate level of safety over their lifecycle. Although both target same issues, their methodology is different in many ways [28]. Such differences in turn may cause misconceptions about the safety requirements and consequently cause mismatch between safety levels from using each standard. Additionally, risk allocation methods used in both standards suffer from inappropriate and uncertain use of subjective expert opinion.

A momentous step before designing safety control system is to determine requirements of SRECS by

[1] Author is with Ecole Polytechnique de Montreal, C.P. 6079, succ Centre-Ville, Montreal (Quebec), H3T 1J4, Canada, (Tel: +1 (403) 667-7324; Email: Mohammad.Sohani@polymtl.ca) (Corresponding Author)
[2] Authors are with Ecole Polytechnique de Montreal, Mohamed-Salah.Ouali@polymtl.ca, Yuvin.Chinniah@polymtl.ca

allocating a required performance level. Poor risk assessment and failure in definition of requirements are responsible for most accidents caused by failures in electrical/electronic safety control systems [6], [28], [27]. An inclusive risk assessment is an important source of information during the design of safety function. The objective is to match the required safety level of SRECS with the level of risk, i.e. if an acceptable risk is achieved only when the SRECS functions properly, the required safety level of the SRECS needs to be proportional to the level of risk. . Similar to risk assessment approaches, the required safety level allocation methods needs evaluation from skilled experts. Experts are asked to evaluate risk parameters using descriptions provided for each risk factor. Since human judgment is never absolute, using expert's opinion to choose between leveled risk parameters is imprecise and uncertain [4]. Heitikko *et al.* [1] showed that results of the required safety level over a particular case might be different based on expertise, experience and background. They formed three groups of engineers from diverse backgrounds and asked them to decide on required safety level for a control system on one machine. The performance levels and safety integrity levels allocated to the safety function varied significantly. Interestingly, it was shown that people tend to select higher risk factors when they are not confident about a parameter. Such doubt necessitates incorporation of expert's uncertainty into elicitation model; otherwise the result would be an overestimation and unnecessary risk reduction, with high costs and complexities in terms of hardware and software.

Using expert judgment is an essential source of information especially when no objective data is available. Since the nature of human judgment is inherently subjective and complex, elicitation of useful information requires a formal methodology. It wasn't until Cooke and Goossens [33], who introduced a comprehensive and systematic methodology for treating expert judgment, that various methods have been proposed to pool, assess and combine experts' opinion. These methods are divided into two major groups: behavioral and mathematical approaches. Mathematical methods have shown better results than behavioral approaches [31]. Transferable belief model (TBM), based on Dempster-Schafer theory of evidence [30], has been employed in various fields such as to find probability distribution in reliability [13], and in environmental studies [14]. TBM is a heuristic model and it evaluates objective and subjective evidence to support a hypothesis. However, due to some restrictions of Dempster-Shafer theorem, this method may show limitations in safety analysis [29]. Probabilistic methods are also used to estimate reliability data [32], and do risk assessment [33]. Bayesian probabilistic approaches are broadly used in data-fusion. Despite interesting results they have shown in elicitation of human judgment, they require multiple sources of data, and are useful when used in human-sensor data fusion approaches. In fact, Bayesian approach models the uncertainty using the probability theory. The meaning of probabilities in modeling expert's opinion in such method is not so obvious [4]. A more promising approach that can deal with imprecision in human opinion and that has been successfully used in modeling reliability [15] and risk assessment [20], [21] is the theory of possibilities. Possibility theory models uncertainty by considering the degree of precision in human reasoning using fuzzy theory. Fuzzy rankings can effectively model uncertainty of individual expert's opinion [25].

The contribution of this paper is to propose a required safety level allocation method using possibility theory to solve two problems, in performance level allocation in ISO 13849 and safety integrity level allocation in IEC 62061, and which are:

1. The subjectivity of using expert opinion to define risk parameters
2. The inconsistency of required safety level allocation between methods in safety standards ISO 13849 and IEC 62061

Using possibility theory, expert is able to evaluate risk parameters in a range of values. As a consequence, instead of one crisp value that demonstrates certitude of evaluation, incertitude can be presented mathematically. Based on the deployed standard, risk allocation rules are fuzzified accordingly

and used to assess fuzzfied risk parameters and allocate required level.

The structure of this paper is as follows: in Section II, conventional methods in both safety standards to define and allocate risk level are discussed. An introduction about fuzzy logic and expert opinion is given in Section III and proposed fuzzy PL allocation is introduced. A case study and results are shown in Section IV. Finally, Section V is dedicated to discussion about the method and results.

II. Conventional Methods in Safety Standards

With popularity of programmable electrical and electronic systems and increasing number of accidents caused by failures in such systems, International Electrotechnical Commission (IEC) and International Standard Organization (ISO) published safety standards over electrical safety systems. IEC 61508 [36] was the first standard to use probabilistic approaches in order to control systematic failures in safety control system. Sector safety standards such as process industry sector (IEC 61511) and machinery sector (IEC 62061) standards were prepared later based on IEC 61508. In 2005, International Standard Organization (ISO) published ISO 13849 by adding probabilistic methods to previous standard EN 954 on machine safety. The standard ISO 13849:2005 added Performance Levels (PLs), to classify safety related control systems, to EN 954 whereas IEC 62061 uses Safety Integrity levels (SILs). Both measurements are based on resistance to faults and safety system's contribution in risk reduction. Performance levels and safety integrity levels are defined in terms of probability of failure per hour (PFH). The emphasis over probabilistic methods in these standards to determine PL and SIL is to control systematic faults and errors. Despite the fact that using such methodologies have dramatically been changed the way safety functions are accepted in industry, there are still problems in using such methods. Most importantly, having two standards running at the same time is not desired by any of standardization groups. In other words, having two different methods to show integrity level of safety function have confused industries and level of understanding among individuals about these systems is not the same.

In both standards, if safety function has to be implemented using SRECS, a detailed specification including Required Performance Level (PL_r) or Safety Integrity Level (SIL) for each SRECS has to be determined. The quantifiable requirements of safety related functions are determined using graphical PL allocation or matrix SIL assignment described in sections A and B.

PFH	PL_r	SIL
$\geq 10^{-5}\ to\ < 10^{-4}$	a	No correspondence
$\geq 3 * 10^{-6}\ to\ < 10^{-5}$	b	1
$\geq 10^{-6}\ to\ < 3 * 10^{-6}$	c	1
$\geq 10^{-7}\ to\ < 10^{-6}$	d	2
$\geq 10^{-8}\ to\ < 10^{-7}$	e	3

Table 1. Relation between PL, SIL and PFH according to ISO 13849 [2] and IEC 62061 [3]

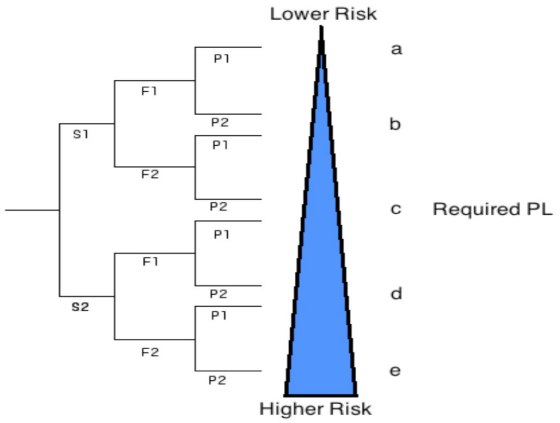


Figure 1. Performance level (PL) allocation according to ISO 13849 []
Severity of injury (S1: reversible injury, S2: irreversible and death),
Frequency and/or exposure to hazard (F1: low, F2: high),
Possibility of avoiding hazard or limiting harm (P1: possible under specific conditions, P2: scarcely possible).

A. Conventional PL assignment in ISO 13849

Three risk parameters, namely: severity of injury (S), frequency and exposure to hazard (F) and possibility of avoiding hazard or limiting harm (P) are defined to assess required performance level as illustrated in Figure 1. Each risk parameter is defined to have two linguistic levels where a description is provided for each level, i.e. S1, S2, F1, F2 and P1, P2. For each risk parameter, two linguistic levels and accordingly descriptions are defined. The severity of injury has two levels of reversible or irreversible. Severity of injury is the most effective parameter to define required PL. As illustrated in the Figure 1, choosing the wrong severity may change PL by two levels. At first glance, choosing between these two levels seems obvious; however this is not true for some cases. i.e., "Is a broken arm reversible or irreversible?" In some cases, people have problem working after suffering from a fracture of the arm because of pain. Of course breaking a rib is different from breaking a finger and yet both may be defined as reversible. The other two parameters, frequency of exposure and possibility of avoiding hazard, have less effect. They also have two levels, such as possible under condition, scarcely, low or high. Using such terms to define levels are difficult to decide.

Despite the simplicity in using risk graph to find PL_r, linguistic terms such as possible, scarcely, reversible, used to describe risk parameters may be interpreted differently among people. In this case, result of risk allocation will be subjective and an SRCS designed based on such safety levels fails to deliver required risk reduction. Human opinion is uncertain and for this reason it is difficult and most of the time inaccurate to associate a situation to one of these two levels. It has also been shown that experts prefer to fix their opinion as intervals instead of a point [4].

The result of conventional PL allocation is performance level, associated with an interval of PFH. In other words, for a wide interval of PFH, performance level remains constant. The ambiguity of information expert use as part of their judgment to find crisp PL intervals affects integrity of the result. This may result to over-design/under-design of the system and consequently higher costs, complexities or safety issues. To eliminate possibility of under-design, standard have used estimations toward the safe side [2] and has increased the requirements for each PL.

B. Conventional SIL assignment in IEC 62061

IEC 62061 employs matrix risk assessment to determine required safety integrity level for an SRECS. In comparison to graphical approach, matrix version is more suitable for computation. According to this standard, the SIL allocation method is informative, so other required SIL allocation methods may be used instead. The standard refers to IEC 61508-5 [36] for other existing techniques. The SIL assignment is done by determination of risk parameters as follows:

1. Severity of injuries (*Se*)
2. Probability of occurrence of harm:
    a. Frequency and duration of exposure (*Fr*)
    b. Probability of occurrence of a hazardous event (*Pr*)
    c. Probability of avoiding or limiting harm (*Av*)

For each of these parameters, numerical values are provided accordingly as in Tables 2 to 5. By using values provided in these tables for risk parameters, *Se, Fr, Pr* and Av are determined and then Table 6 is used to find SIL value. The probability of harm is determined by summation of last three parameters (2-a to 2-c):

$$Cl = F_r + P_r + A_v \tag{1}$$

Table 6 illustrates SIL assignment according to IEC 62061. For each SIL, a PL can be associated using Table 1. The relation between PL and SIL is based on maximum tolerable probability of dangerous failure per hour, i.e., severity value of 3 and *Cl* of 9 assigns SIL 1, which is equal to PFH= $[10^{-6}, 10^{-5}]$, and according to Table 1 is equal to PL_b or PL_c.

Consequences	Severity Value (Se)
Irreversible: death, losing an eye or arm	4
Irreversible: broken limb(s), losing a finger	3
Reversible: requiring attention from a medical practitioner	2
Reversible: requiring first aid	1

Table 2. Classification of severity of harm (Se) according to IEC 62061 [?]

Frequency of occurrence	Frequency Value (Fr)
≤ 1 per hour	5
< 1 per h to ≥ 1 per day	5
< per day to ≥ 1 per 2 weeks	4
< 1 per 2 weeks to ≥ 1 per year	3
< 1 per year	2

Table 3. Classification of frequency of occurrence (Fr) according to IEC 62061 [?]

Probability of occurrence	Probability Value (Pr)
Very high	5
Likely	4
Possible	3
Rarely	2
Negligible	1

Table 4. Classification of probability of occurrence (Pr) according to IEC 62061 [?]

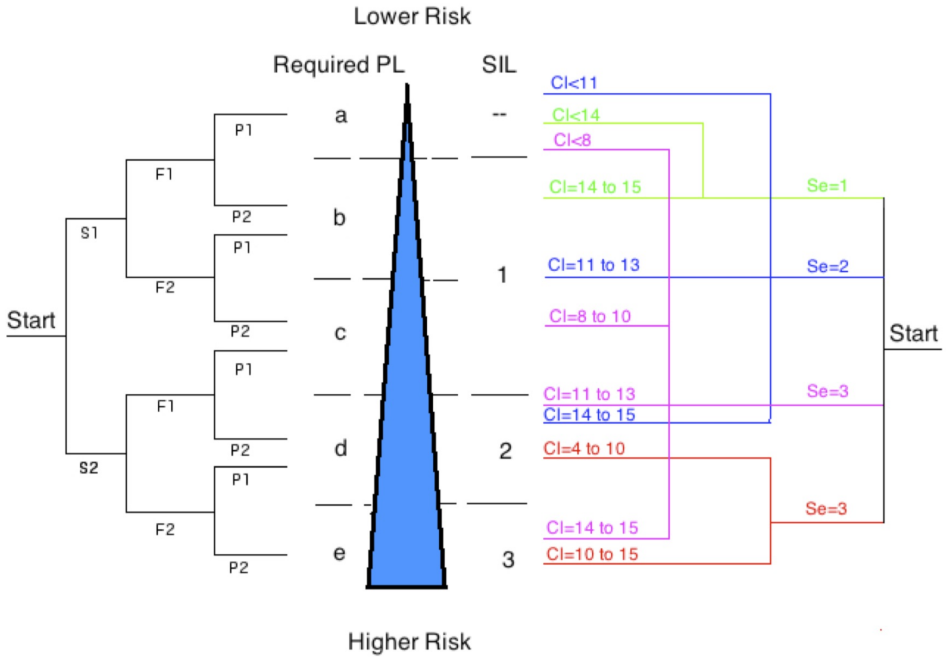


Figure 2. SIL allocation and relationship between PL and SIL. From left to right: PL allocation. From right to left: SIL allocation.

Probability of avoiding harm	Probability value (Av)
Impossible	5
Rarely	3
Probable	1

Table 5. Classification of probability of avoiding or limiting harm (Av) according to IEC 62061

Severity (Se)	Class (CL)				
	4	**5-7**	**8-10**	**11-13**	**14-15**
4	SIL 2 PLd	SIL 2 PLd	SIL 2 PLd	SIL 3 PL e	SIL 3 PL e
3			SIL 1 PL b/PL c	SIL 2 PL d	SIL 3 PL e
2				SIL 1 PL b/PL c	SIL 2 PL d
1					SIL 1 PL b/PL c

Table 6. SIL assignment matrix based on IEC 62061, Annex A [?] and its PL value according to Table 1

C. Relationship between PL and SIL

The relation between PL allocation in ISO 13849 and SIL assignment in IEC 62061 in Table 1 suggests that required SIL and PL for a safety function have to be equal with respect to PFH, regardless of which safety standard is used. In other words, using Table 1 to transfer results between PL and SIL should give the same result as using PL and SIL allocation independently. However, it can be shown that in practice,

relationship in Table 1 does not hold for some cases (see Figure 2) . The following points can be mentioned as reasons:

1) Number of risk parameters are different

First difference between safety allocation methods is in number of risk parameters used in each standard. The matrix SIL assignment method uses four risk parameters while graphical PL allocation uses three risk parameters. In fact, probability of occurrence is not considered in PL allocation method. Thus, it can be said that PL allocation method does not distinct between "probable" and "rare" situations. According to IEC 62061, influential parameters to estimate the probability of occurrence of hazard are machines conduct in different modes of operation and human interaction with the machine [3]. For example based on this approach, unexpected human error because of stress can increase probability of occurrence. However, PL allocation does not consider such influence.

2) Number of levels for each parameter

Another difference between two methods is in number of levels determined for each risk parameter. Risk parameters in ISO 13849 have two levels, while in IEC 62061, 3 to 5 levels are used for each risk parameter. Increasing levels for parameter enables experts to associate detailed description to a hazard; however, it also increases the complexity. To compare the two methods, matrix SIL allocation can be illustrated as a graph (See Figure 2). In this graph, from right to left in the left SIL allocation is illustrated, where risk factor "P_r" is considered to be equal to 5. In fact, the worst case is considered. In this figure, the column from right to left shows SIL values for different values of S_e, F_r and A_v. Each SIL may be associated to a situation. It can be seen that for some cases, no SIL value is recommended. To find the associated PL, the following approaches exist:

1. To use Table 1 and equate each SIL to a PL based on PFH
2. Start with method in ISO 13849 and find required PL by determining *S, F* and *P.*

Subsequently, if PL has to be allocated using approach 2 for each of situations in Table 2, S, F and P have to be determined. Subsequently, the following values for each risk parameter may be estimated. Severity of risk consequence in SIL assignment is divided into four categories: *Se=1* and *Se=2* are associated to reversible situations and *Se=3* and *Se=4* are associated to irreversible situations. In PL allocation (Figure 1) however, severity has two categories: reversible (S1) and irreversible (S2). This implies that *Se=1* and *Se=2* are equal to *S1* and *Se=3* and *Se=4* are equal to *S2*. The same procedure for frequency of exposure and probability of avoidance result the following equations:

1. $Se = 1{,}2 \rightarrow S = S1, Se = 3{,}4 \rightarrow S = S2$ (2)
2. $Fr = 2{,}3 \rightarrow F = F1, Fr = 4{,}5 \rightarrow F = F2$ (3)
3. $Av = 1 \rightarrow P = P1, Av = 3{,}5 \rightarrow P = P2$ (4)

The second column in Figure 2 shows PL value using equations 1 to 3 above. As an example, if *Se=2*, *Fr=5, Av=5* and *Pr=5*, then SIL 2 is assigned to the safety control system. However, for the same SRECS, *S=S1, F=F2* and *P=P2* and consequently, *PL=PLc*. According to Table 1, SIL 2 is at the same level of safety as PL d and this may be considered as overdesign based on SIL or under design based on PL.

III. Fuzzy Risk Allocation and Validation

A. Fuzzy sets

Fuzzy logic and fuzzy sets establish one of the most influential notions in engineering and science [10], [11], [37], [5], [26]. The intuitive and transparent concept of fuzzy set emulates how the real world is perceived and described by human. Fuzzy is proven to be a powerful tool to model nonlinear, complex and ill-defined systems [9]. In contrast to conventional modeling approaches, fuzzy logic is based on human reasoning abilities in complex and imprecise environment [12]. As a result, unlike other modeling tools that require accurate equations to model real world problems, fuzzy can deal with existing ambiguities in human driven measurements and using inaccurate information, which exist in most real world problems.

Fuzzy has been successfully applied to problems in control theory [10], [11], medicine [13], [14], [16], modeling nonlinear systems [15], image processing [22] and many other areas of research.

In fuzzy modeling, membership functions (MFs) are used to interpret expert's knowledge or incorporate imprecise information into mathematical model. MFs represent the degree of truth or degree to which an element belongs to a set. A fuzzy set *A* in the universe of discourse *X* is defined as:

$$A = \{x, \mu_A(x) | x \in X\} \tag{5}$$

where $\mu_A(x) \in [0,1]$ is the membership function of *x* in *A*. The advantage of fuzzy comes from the fact that unlike conventional set theory, *x* may "partially" belong to a set by assigning a value between zero and one. Two important properties of MFs are normality and unimodality [9]. Triangle and trapezoid are two popular piecewise-linear membership functions, with these two properties, that have been successfully used in various problems [10]. Triangular MFs are equal to 1 at one point and are used to model linguistic terms such as "He is around 6 feet". Having a flat top equal to 1, trapezoidal functions are suitable to model linguistic terms such as "It feels cold". The term cold is vague and can be attributed to a range of degrees.

Fuzzy inputs are mapped to output functions by passing through Fuzzy logic Inference Systems (FIS). Two most popular fuzzy inference methods are Mamdani [23] and Takagi-Sugeno (TSK) [24]. The Mamdani fuzzy inference system is the most employed rule-based method. A collection of fuzzy IF-THEN rules are employed by the fuzzy inference engine to determine mapping from the input fuzzy set $U \subset R^{\varsigma}$ to output set $V \subset R^{\eta}$. For given set of $\{(x_p, y_p) | x_p \in R^{\varsigma}, y_p \in R^{\eta}\}$, IF-THEN rules in Mamdani model with n_r rules are defined as:

$$R^i: IF\ x\ is\ A_i, THEN\ y\ is\ B_i, i = 1, \dots, n_r \tag{6}$$

where $A_i = \{A_i^1, A_i^2, \dots, A_i^{\varsigma}\}, B_i = \{B_i^1, B_i^2, \dots, B_i^{\eta}\}$ are input and output fuzzy sets respectively. The aggregation of fuzzy rules used in this method is a way to employ T-norm and T-conorm operators [10] in order to unite input fuzzy sets and produce a single output. If A_i and B_i are fuzzy sub-sets, intersection ($C = A \cap B$) and union ($C = A \cup B$) operators are defined as:

$$\mu_{inter}(x) = T_{\cap}(\mu_A(x), \mu_B(x)) \tag{7}$$
$$\mu_{uni}(x) = T_{\cup}(\mu_A(x), \mu_B(x)) \tag{8}$$

where $T_{\cap}$ and $T_{\cup}$ are intersection and union operators respectively. In this respect, any operator with T-norm and T-conorm properties may be used, while "algebraic product" and "min" are standard intersection operators and "algebraic sum" and "max" are considered as two standard union operators [11]. The last step in FIS is to transform the output fuzzy set into a crisp value. Centroid-defuzzification or center of gravity, which resembles the center of mass formula from mechanics, is the most extensive approach to defuzzify the output:

$$\bar{u} = \frac{\int u.\mu(u)du}{\int \mu(u)du} \tag{9}$$

B. Fuzzy PL allocation

The PL allocation in the standard comprises of two steps: ranking risk parameters from expert's judgment and PL allocation based on graphical approach (see Figure 3). Risk parameters are defined based on the risk allocation of the standard (Figure 3, right) and then expert introduces his opinion (Figure 3, left) to rank the rules from risk allocation graph to form the input to the fuzzy system. Fuzzy distributions, described as fuzzy rankings in [25], can effectively model existing uncertainty in expert's opinion. Following subsections discuss development of fuzzy ranking functions and fuzzy risk parameters.

1) Expert's opinion

Due to the nature of risk estimation methods, expert judgment elicitation is an essential part of all risk assessment and performance level allocation methodologies. Expert judgment is used in other areas such as reliability analysis [13] and knowledge acquisition [12] and climate analysis [14] as an integral part of input information. In machine safety, however, expert judgment is the sole way to assess risk parameters, which in turn are essential to find requirements of safety level. Based on the type of risk assessment and allocation method, the opinion can also come in various formats such as numbers, graphical grades, or words (descriptions). These imply that to acquire valid result, elicitation method has to be designed carefully by considering type of information used and the purpose of elicitation. Each technique has its own advantages and disadvantages and different factors may affect the plausibility of the results. Deciding on how many experts may participate, expert's background, the level of interaction among them, it has to be done in groups or individually and whether the level of experience is a factor, may affect validity of the results [33].

In elicitation problems, often one or more experts are asked to present their opinion for each parameter [8]. Elicitation of expert opinion is a valuable source of information in decision-making problems and is used in risk analysis [7]. Expert opinion may have different forms. Accordingly, a questionnaire has to be designed appropriate to elicitation method. The questionnaire may include points with absolute descriptions in contrast with relative descriptions. Normally, experts are asked to choose a point that mostly describes the situation. However, a single point means that expert has to be sure about his opinion and only specified descriptions may be chosen. This type of elicitation is rather simple but it does not cover the vagueness in human opinion. It is more proper to ask expert to present his opinion as degrees for each parameter. In a more advanced approach by using possibility theory and asking opinion in shape of a triangle or trapezoidal function, expert is able to give vague opinion about parameters. Fuzzy weighting is a useful approach with low number of experts [25]. This method of elicitation has been used successfully in reliability problems. Using this method in PL allocation, expert's judgment is expressed as a function, such as triangle or trapezoid, which is used to rank risk factors from graphical PL allocation (Figure 4). Fuzzy ranking functions have been used in risk assessment methods to solve the subjectivity of expert's opinion. Nait-Said *et al.* [20] have used fuzzy logic to propose an alteration to risk assessment in IEC 61508. They showed that by developing fuzzy SIL allocation, rules in the risk graph are preserved while using linguistic values to assess the risk can improve the results. Simon *et al.* [21] used fuzzy ranking functions to elicit and aggregate expert opinion and improve the SIL allocation. They used possibility theory proposed by Sandri and Dubois [4] to create fuzzy risk graph for IEC 61508. In an example, they showed that using expert opinion with risk reduction distribution instead of conventional risk allocation could make the results more promising. We use the possibility distribution not only to improve elicitation of expert's opinion, but also to decrease the existing distance between results of PL and SIL allocation. Using descriptions for risk parameters of SIL allocation, and develop a new fuzzy questionnaire for PL allocation can do this.

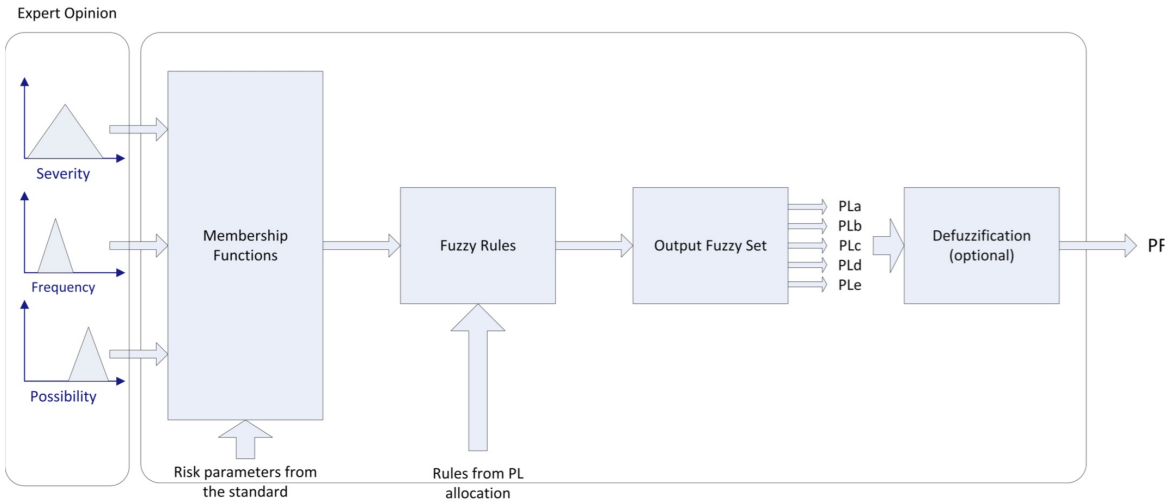


Figure 3. Fuzzy PL allocation; composed of expert opinion and fuzzy PL allocation.

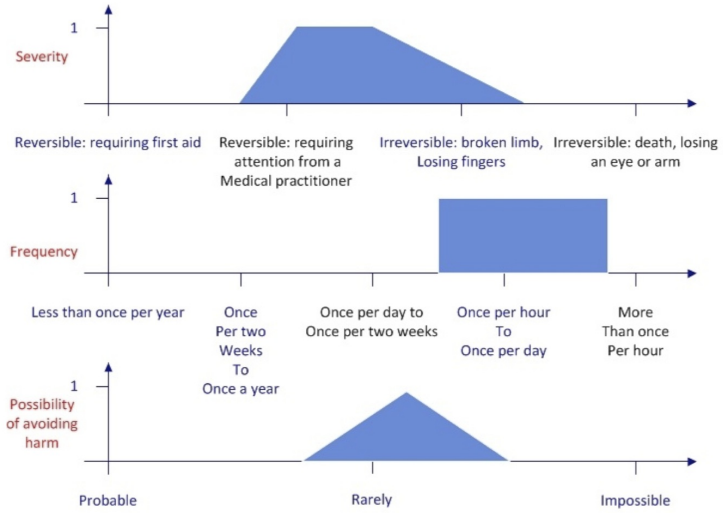


Figure 4. Fuzzy PL allocation; composed of expert opinion and fuzzy PL allocation.

The method used here is based on fuzzy logic and is developed by Sandri and Dubois [4] and Page *et al.* [25]. It has been used in reliability [15], data fusion [16], [17], infrastructure safety [18], risk management [19] and risk analysis [20], [21].
An aggregation is required to rank fuzzy membership functions:

$$\mu_{R_i'} = S(\zeta_o(x) \odot \mu_{R_i}(x)) \tag{10}$$

where ζ_o is the function representing expert's judgment, μ_{R_i} is the risk parameter's membership function, S is any T-conorm and $\odot$ is T-norm function. T-norm functions are used as intersection functions. Two popular t-norms are minimum and algebraic product [11]. Minimum function is accepted as T-norm and is

useful in many applications, however, it priories one value over the other. Thus, algebraic product is preferred here. T-norm functions are used as union functions. Maximum function is a common simple way to implement T-norm.

Figure 3 illustrates the results of the developed questionnaire for PL allocation. It is developed based on possibility theory and using descriptions in IEC 62061. This way, risk factors in PL allocation are ranked based on descriptions in SIL allocation while rules remain the same. This implies that risk factors can have values other than crisp low, high values.

2) Fuzzy risk parameters

The universe of discourse for each risk parameter level $R_i = \{S_i, F_i, P_i\}$, $i=1,2$ is defined as X=[0,1]. Owing to the allocation rules in the standard, only two MFs, associated with R_i, i=1,2, may be defined for each risk parameters. Otherwise, more rules are required for each MF, which entails alteration of the rules in standard. From graphical risk assessment it can be deduced that: R_1 has full membership at zero and R_2 has its full membership at one. For fuzzified risk parameters, values between zero and one are partially member of R_1 and R_2. Moving x from zero toward one, membership value of R_1 is decreasing so μ_{R_1} is monotonically decreasing function, for R_2 however, membership function has to be monotonically increasing. Linear MFs are used for each R_i to incorporate gradual transition:

$$\mu_{R_1}(x) = \{-x + 1 | 0 \leq x \leq 1\} \quad (11)$$

$$\mu_{R_2}(x) = \{x | 0 \leq x \leq 1\} \quad (12)$$

Each MF is aggregated using formula $\{\mu_{R_i'} = S(\zeta_o(x) \odot \mu_{R_i}(x))\}$ and form input to fuzzy inference system. The aggregation is done as follows:

$$\mu_{R_1'}(x) = \max\{\zeta_o(x) \times (-x + 1)\}, \text{for } 0 \leq \text{x} \leq 1 \quad (13)$$

$$\mu_{R_2'}(x) = \max\{\zeta_o(x) \times x\}, \text{for } 0 \leq \text{x} \leq 1 \quad (14)$$

The first step in inference system is applying IF-THEN rules. IF-THEN rules from graphical risk allocation are shown in Table 4. Since all these rules include intersection combination, min function is deployed as T-norm function. Results from fuzzy rules are truncated using min function. For each rule, input to implication process is a fuzzy number and output is an associated fuzzy set. Two functions usually used as implication are min and product. The former truncates and the later scales the output fuzzy number.

	Severity		Frequency		Possibility		PL
1	S1	AND	F1	AND	P1	=>	a
2	S1	AND	F1	AND	P2	=>	b
3	S1	AND	F2	AND	P1	=>	b
4	S1	AND	F2	AND	P2	=>	c
5	S2	AND	F1	AND	P1	=>	c
6	S2	AND	F1	AND	P2	=>	d
7	S2	AND	F2	AND	P1	=>	d
8	S2	AND	F2	AND	P2	=>	e

Table 7. IF-THEN rules based on PLr allocation rules in the standard

Output from fuzzy inference can be defined as five elements in a set: $PL_r = (PL_a, PL_b, PL_c, PL_d, PL_e)$. Each value shows the degree of corresponding performance level. These values can then be discussed among safety engineers and designers to find the performance level.

IV. Results

Functionality and improvements that fuzzy logic appends to machine safety standards will be studied using a case study. The aim here is to compare results from conventional approach versus the ones from proposed approach and show how the proposed fuzzy allocation results from ISO 13849 are more comparable with the ones from ISO 62061. The machine under study is a small plastic injection-molding machine. It is a hydraulic- press with maximum 350 kN closing force. The machine is designed to produce parts by forcing plastic pellets into a heated barrel, melting them and injecting the molten plastic under pressure into a mold cavity before cooling them down. The cooling process causes the plastic material to take the shape of the mold and the parts are then ejected. The following specifications are considered for this machine:

- It is an automated machine, which can be operated on the semi-automatic mode, i.e. operator reached into mold area at end of each cycle to manually remove the plastic part.
- Each cycle takes from 10*sec* to 90*sec* depending on shape and type of mold and product
- After each cycle, operator has to take the product out from the molding space
- The operator of the machine is supposed to be trained and know how to operate the machine well enough. Operator is familiar with all commands and how the machine works in different cycles.

The machine is designed for industrial use and is supposed to work in the following situation:

- Machine is working 365 days a year
- It works 8 hours a day in one shift
- Each cycle is supposed to take 60sec

If no safeguard is designed for the operator, he can access the press and molding part.

Using IEC 62061 and ISO 13849 for molding machine is more a theoretical case study to illustrate comparability of results from new method to both safety standards. The EN 201 [38], safety standard for injection molding machine, allocates a PL equal to e for mold hazardous area. Additionally, plastic molding machine is a combination of electric and hydraulic devices, which makes ISO 13849 a more appropriate standard. However, as a theoretical study, it is not in appropriate to use ISO 13849 for hydraulic parts and IEC 62061 for electrical parts.

Regarding the aforementioned specifications for the molding machine, risk parameters may be estimated as follows:

1) Severity

Like other types of presses, the injection molding press is dangerous enough to crush upper limbs or cut fingers or part of hand exposed to the molding area. However, considering small size of machine for this study and that operator is familiar with machine, it is supposed that only his hand is exposed to the hazardous area (i.e. the molding zone) and probability of death is negligible. As a consequence, despite the fact that the result would not be death, severity of harm is:

- SIL: Irreversible risk: broken limb, loosing finger, Se = 3
- PL: S=S2.

However, using fuzzy ranking functions, an expert may correspond his opinion as in Figure 5-a.

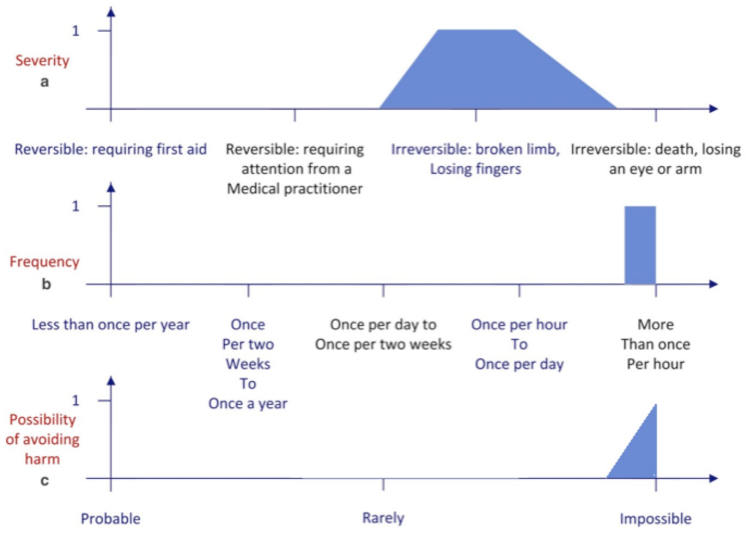


Figure 5. IF-THEN rules based on PLr allocation rules in the standard

2) Frequency and/or exposure to hazard

Machine is working 8 hours a day and each cycle is supposed to take no longer than 90sec. In such case:

- SIL: Fr is more than once per hour, Fr = 5
- PL: F=F2

Function that an expert may propose for such case is shown in Figure 5-b. Expert considers the frequency to be in between more than once per hour and points nearby with equal possibility.

3) Possibility of avoiding hazard or limiting harm

The machine is too fast to make it impossible for an operator to avoid harm. Even if the operator has the right training, it is impossible he can take his hand out of dangerous zone. So, the probability can be considered as impossible.

- SIL: Rare, Av=5.
- PL: P=P2.

Figure 5-c illustrates a possible proposition for this case based on possibility theory.

4) Probability of occurrence of a hazardous event

As suggested in IEC-62061, risk parameters are chosen regardless of what value has been assigned to other parameters. Standard notes that probability of occurrence of a hazardous event depends on workspace, interaction between operator and machine and his behavior. Having the assumption that operator has the right training; the probability of occurrence of hazard can be set to probable, equal to 3.

With such ranking functions illustrated in Table 6, SIL level is equal to:

$$Cl = F_r + P_r + A_v = 5 + 3 + 5 = 13 \rightarrow SIL = 2$$

While based on the parameters "*S=S2, F=F2* and *P=P2*" PL is equal to PLe, based on PFH (see Table 1) SIL=2 and PLe are not in the same range. As a matter of fact, SIL=2 is at the same level as PLd. Now using possibility theory, risks parameters can be presented as in Figure 5:

$$\mu_{R_1'}(x) = \max\{\zeta_o(x) \times (-x + 1)\}, \text{for } 0 \leq x \leq 1$$
$$\mu_{R_2'}(x) = \max\{\zeta_o(x) \times x\}, \text{for } 0 \leq x \leq 1$$

where $\zeta_o(x)$ is considered to be functions in Figure 5. Risk parameters calculated from ranking functions mentioned are:

$$Severity(\mu_{R_1'}(x), \mu_{R_2'}(x)) = (0.48, 0.71)$$
$$Frequency\ of\ exposure(\mu_{R_1'}(x), \mu_{R_2'}(x)) = (0.04, 1)$$
$$Possibility\ of\ Avoidance(\mu_{R_1'}(x), \mu_{R_2'}(x)) = (0.17, 1)$$

	Severity		Frequency		Possibility		PL
1	0.48	AND	0.04	AND	0.17	=>	0.04 a
2	0.48	AND	0.04	AND	1	=>	0.04 b
3	0.48	AND	1	AND	0.17	=>	0.17 b
4	0.48	AND	1	AND	1	=>	0.48 c
5	0.71	AND	0.04	AND	0.17	=>	0.04 c
6	0.71	AND	0.04	AND	1	=>	0.04 d
7	0.71	AND	1	AND	0.17	=>	0.17 d
8	0.71	AND	1	AND	1	=>	0.71 e

Table 8. IF-THEN rules based on PLr allocation rules in the standard

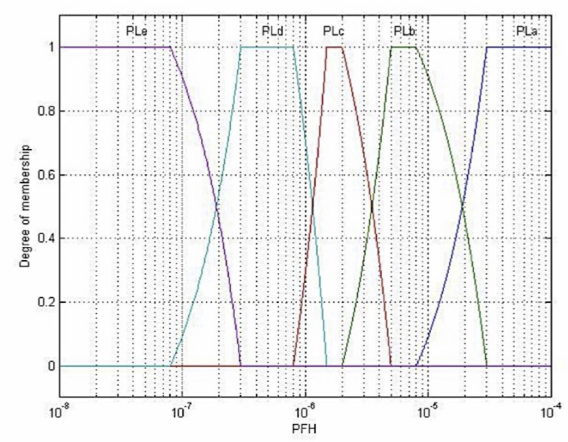


Figure 6. De-fuzzification functions

Using center of gravity as de-fuzzification method and de-fuzzification functions of Figure 6 in Matlab, the performance level (*PL*) is equal to d, which is at the same level as *SIL=2*. Using the same method to find SIL, SIL will be equal to 2. Thus, using fuzzy sets theory enables experts to give opinions that are uncertain and contain vagueness. It also solves the problem of inconsistency between results in the two standards to some extent. The result of fuzzy inference used is dependent on the de-fuzzification function used.

Another possible option to find PL level in the above case study is to use Table 6 and discuss it among experts and choose the most appropriate level. It can be discussed that the result should be chosen between PLd and PLe. The coefficient in Table 8 suggests that PLe is more probable. Discussing risk parameters also backs up the same theory. However, if a mean approach is used, since PLc and PLb have coefficients, they change possible result from PLe to PLd. Unfortunately, the result of fuzzy approach is dependent on de-fuzzification method and functions. Changing de-fuzzification functions may change the result by two levels.

V. Conclusion

A fuzzy performance level allocation is proposed to solve two major problems that exist with conventional methodology. One problem with conventional PL allocation is subjectivity of using expert's opinion. Possibility theory can deal effectively with subjectivity by using linguistic values and fuzzy

ranking functions. Instead of transferring thought to two crisp levels, expert is capable to present his idea as a function, representing his vague opinion.

Another issue with performance level allocation is that required PL using ISO 13849 is not always in compliance with SIL from IEC 62061. The proposed approach can also deal with this problem by using levels used in risk parameters of IEC 62061 in PL allocation. Since levels in SIL allocation are more inclusive, using them in allocating PL can solve to some extent the problem. However, as other fuzzy approaches, result depends extensively on how the fuzzy system is designed.

One issue with using fuzzy logic is to set membership and de-fuzzification functions. Membership functions used in this approach have the simplest shape, linear between two possible end points, while, non-linear MFs such as sigmoidal can be considered. Defuzzification method may be discussed among experts to choose the most appropriate PL for a safety function. A method to set de-fuzzification function is to use neuro-fuzzy system. A set of safety functions with known PLs can be presented to the neural network that learns the nonlinear function and can then help to choose de-fuzzification function parameters by decreasing error between the results.

Another point to consider is the reliability of experts. This may be solved by presenting problems with known answers to experts and then using nonlinear functions to interpret their opinion. A tolerance level can also be set for acceptance of opinion. If opinion passes this level, the expert can be categorized as invalid and unreliable.

Using expert systems in critical decision making problems are more informative approaches rather than reliable final decision making approaches. The fuzzy approach can be an informative approach to help experts in allocating PL and SIL to a safety related control system. It can decrease the ambiguity of results from safety standards, especially when results vary. . As mentioned earlier, the result of using possibility theory can help to improve the choice of required safety levels..

REFERENCES

[1] M. Hietikko, T. Malm, J. Alanen, "Risk estimation studies in the context of a machine control function," *Journal of Reliability Engineering and System Safety,* Vol 96, 2011, pp. 767-774.

[2] "ISO 13849-1, Safety of machinery – safety related parts of control systems – Part I, general principles for design," *International Standard Organization (ISO),* 1999.

[3] "IEC 62061 ed1.0, Safety of machinery – Functional safety of safety related electrical, electronic and programmable electronic control systems," *International Electrotechnical Commission,* 2005.

[4] S. Sandri, D. Dubois, "Elicitation, Assessment and Pooling of Expert Judgment Using Possibility Theory," *IEEE Transaction on Fuzzy Systems,* Vol. 3, No. 3, August 1995, pp. 313-335.

[5] L.A. Zadeh, "Fuzzy sets as a basis for a theory of possibility," *Fuzzy Sets and Systems,* Elsevier, 1999, pp. 9-34.

[6] R. Piggin, "What's happening with machine safety standards and networks?", *Assembly Automation,* Emerald Automation, Vol 26, Num. 2, 2006, pp. 104-110.

[7] M.A. Meyer, J.M. Booker, "Eliciting and Analyzing Expert Judgment: a Practical Guide.", *Academic Press,* London, UK.

[8] M.M. Granger, L. Pitelka, E. Shevliakova, "Elicitation of expert judgment of climate change impacts on forest ecosystems," *Climate change,* 49 (3), pp 279-307, 2001.

[9] M.Y Chow, S. Altrug, H.J Trussell, "Heuristic constraints enforcement for training of and knowledge extraction from a fuzzy/neural architecture – Part I: Foundations," *IEEE Transaction on Fizzy Systems,* 7(2), pp 143-150, 1999.

[10] Y. Wu, B. Zhang, J. Lu, K.L. Du, "Fuzzy logic and neuro-fuzzy systems: a systematic introduction", *International Journal of Artificial Intelligence and Expert systems (IJAE),* Vol. 2, Issu (2), 2011.

[11] J.J. Buckley, E. Eslami, "An introduction to fuzzy logic and fuzzy sets," Heidelberg: Physica-Verlag, 2002.

[12] M.A. Meyer, J.M. Booker, "Eliciting and analysis expert judgment: a practical guide," *Academic Press*, London, UK, 1991.

[13] P. Smets, "The transferable belief model for expert judgment and reliability problems", Reliability engineering and Systems Safety, Vol. 38, Issue 1-2, 1992, pp. 59-66.

[14] M. H. Duong, "Hierarchical fusion of expert opinions in the transferable belief model, application to climate sensitivity," International Journal of Approximate Reasoning, Vol 49, 2005, pp. 555-574.

[15] F. Delmotte, "Modeling of reliability with possibility theory," *IEEE Transaction on Systems, Man and Cybernetics, Part A: Systems and Humans,* Vol 28., Issue 1., pp. 78-88.

[16] S. Destercke, "Possibilistic information fusion using maximal coherent subsets", *IEEE Trans. on Fuzzy Systems,* vol 17, Issue 1, 2009, pp. 79-92.

[17] J. Gebhardt, R. Kruse, "Parallel combination of information sources," *Handbook of Defeasible Reasoning and Uncertainty Management Systems,* Springer, Vol. 3, 1998, pp 393-439.

[18] N. Rosmuller, G. E.G Beroggi, "Group decision making in infrastructure safety planning", *Journal of Safety Science,* Elsevier, Vol. 42, Issue 4, 2004, pp. 325-349.

[19] G.E.G Beroggi, "Multi-expert operational risk management", *IEEE Trans. on Systems, Man , and Cybernetics,* Vol. 30, Issue 1., 2000, pp. 32-44.

[20] R. Nait-Said, F. Zidani, N. Ouzraoui, "Modified risk graph method using fuzzy rule-based approach," *Journal of Hazardous Materials,* Elsevier, Vol. 164, Iss. 2-3, 2009, pp. 651-658.

[21] C. Simon, M. Sallak, J.F. Aubry, "Allocation de SIL par agrégation d'avis d'experts," *15e Congrès de Maîtrise des Risques et de Sûreté de Fonctionnement*, Lille : France (2006)

[22] I. Bloch, "On fuzzy distances and their use in image processing under imprecision", *The Journal of Pattern Recognition,* 32, 1999, pp. 1837-1895.

[23] Mamdani, E.H. and S. Assilian, "An experiment in linguistic synthesis with a fuzzy logic controller," *International Journal of Man-Machine Studies*, Vol. 7, No. 1, pp. 1-13, 1975.

[24] T. Takagi, M. Sugeno, "Fuzzy identification of systems and its applications to modeling and control," *IEEE Trans. on Systems, Man, and Cybernetics,* Vol. 15, No. 1, 1985.

[25] T. Page, A.L. Heathwaite, L.J. Thompson, L. Pope, R. Willows, "Eliciting fuzzy distributions from experts for ranking conceptual risk model components", *Journal of Environmental Modeling and Software,* Elsevier, Vol. 36, 2012, pp. 19-34.

[26] K. M. Passino, S. Yurkovich, "Fuzzy Control," *Addison Wesley,* Menlo Park, USA, 1998.

[27] T. Fukuda, M. Hirayama, N. Kasai, K. Sekine, "Evaluation of operative reliability of safety-related part of control system of machine and safety level," *SICE Annual Conference,* Kagawa University, Japan, 2007.

[28] P. Lereverend, "Inside the standardization jungle: IEC 62061 and ISO 13849-1, complementary or competing?" *5th Petroleum and Chemical Industry Conference Europe – Electrical and Instrumentation Applications*, 2008.

[29] D. Gerts, "A transferable belief model representation for physical security of nuclear materials," Report, Idaho National Laboratory, US, 2010.

[30] G. Shafer, "A mathematical theory of evidence," *Princton University Press,* Princston, NJ, 1976.

[31] F. Ouchi, "A literature review in the use of expert opinion in probabilistic risk analysis," Technical Report 3201, World Bank, 2004.

[32] S. Campodonico, N.D. Singpurwalla, "Inference and predictions from poisson point process incorporating expert knowledge," *Journal of the American Statistical Association,* Vol. 90, Issue 429, pp. 220-226, 1995.

[33] R.M. Cooke, L.H.J. Goossens, "Procedures guide for structured expert judgment in accident consequence modeling," *Radiation Protection and Dosimetry,* Vol. 90, No. 3, pp. 303-309, 2000.

[34] F. Donauer, "Integrated safety in converters: Functional safety with modern AC drives", *Mechatronik,* Vol. 120, No. 5, 2012, pp 20-21,

[35] R. Piggin, "What's happening with machine safety standards and netwroks?", *Assembly Automation,* Vol. 26, No. 2, 2006, pp 104-110.

[36] "IEC 61508-1/7, Functional safety of electrical/electronic/programmable electronic safety-related systems", International Electrotechnical Commission, 2010.

[37] M. Sohani, K.K. Khosrovian, B. Makki, A. Riazati, N. Sadati, "A Neuro-Fuzzy Approach to Diagnosis of Neonatal Jaundice", *Proc. BIONETICS 06,* Italy, 2006.

[38] "BS EN 201:2009, Plastic and rubber machines. Injection molding machines. Safety requirements", *British standard Institute,* 2009.